all rights reversed

HACKER

season 05 / issue 01

τεύχος 049 - Κάστανα Ζεστά Edition

Το δικό σας cloud με το openSUSE [*]

Η ζωή με έναν OpenVPN-enabled router

Virtualization με το KVM, στο openSUSE

Εντοπισμός και περιορισμός των bandwidth hogs

Κρυπτογράφηση αρχείων πριν ανέβουν στο σύννεφο

Βασικές ρυθμίσεις μετά την εγκατάσταση του openSUSE

[*] ...ακόμη κι αν έχετε ταπεινό hardware

all rights reversed

HACKER


CMYK & WEB
cmykandweb.gr
GRAPHIC DESIGN
design • layout • web

Εκδότης / Διευθυντής	Χρήστος Βαρελάς
Αρχισυντάκτης	Παναγιώτης Βαρελάς
Σύμβουλοι έκδοσης	Νίκος Μουρατίδης, Βούλα Παυλίδου
Σύνταξη	Παναγιώτης Βαρελάς, Χρήστος Βαρελάς, Γιώργος Γιάννου, Μανώλης Κιαγιάς, Πέτρος Κυλαδίτης, Νίκος Μουρατίδης, Θωμάς Σερμπίνης, Μέσος Παπαδόπουλος (TM), Χρίστος Τόμπρας, @arkoudos
Γραμματική επιμέλεια	Βούλα Παυλίδου
Καλλιτεχνική Επιμέλεια	Πέτρος Φιλιππίδης

Το ηλεκτρονικό περιοδικό deltaHacker είναι συνδρομητικό και εκδίδεται από την Parabing Creations δώδεκα φορές το χρόνο, κάθε μήνα. Η Parabing Creations έχει την έδρα της στην Καλαμαριά Θεσσαλονίκης. Ο δικτυακός τόπος του περιοδικού είναι στο http://deltahacker.gr. Το email επικοινωνίας είναι το talk2us@deltahacker.gr και ειδικά για τις συνδρομές είναι το subscriptions@deltahacker.gr. Οι γενικές πληροφορίες για τις συνδρομές παρατίθενται στο http://deltahacker.gr/pdf12order και από την ίδια σελίδα γίνονται οι παραγγελίες συνδρομών.


deltaHacker Field Bag
€25.50
MORE COLORS AVAILABLE
deltaHacker Mugs
€12.50
deltaHacker Thermos® Can Cooler
€17.50
QUESTIONS?
ORDER BY PHONE?
CALL 1-877-809-1659
Where's My Stuff?
Track your recent orders.
View or change your order.
Shipping & Returns
See our shipping rates.
Make a return or exchange.
Need Help?
Satisfaction Guaranteed.
Visit our Customer Service.
CafePress.com. All rights reserved.
Δώρα με στιλ, που έχουν *αληθινή* αξία.
Όλα στο μαγαζάκι του deltaHacker,
κάτω από το Cafepress.
Περάστε μια βόλτα από το
http://www.cafepress.co.uk/deltahacker
–σας περιμένουμε!

Θέσεις 27 και 28

του Χρήστου Βαρελά

Φίλες και φίλοι,

- Σας γράφω τούτες τις γραμμές μέσα από λεωφορείο του ΚΤΕΛ, καθ' οδόν προς Δράμα. Δίπλα μου είναι η κα Σύμβουλος Εκδόσεως (TM) του περιοδικού, η οποία πριν από λίγο άκουγε μουσική από ένα μπλε MP3 player που έχει μαζί της. Τώρα προσπαθεί να βγάλει φωτογραφίες με το κινητό της -- κι ας είναι χαμηλός ο φωτισμός.
- Περνάμε από το Λόφο Καστά, στην Αμφίπολη, κι όποτε είμαστε εδώ κοντά η κα Σύμβουλος Εκδόσεως (TM) συνηθίζει να βγάζει φωτογραφίες.
- Απόψε προσπαθεί και να *μη* σχολιάσει το γεγονός της ξαφνικής ανάσυρσης του laptop από το σακίδιό μου, βεβαίως και της προσπάθειάς μου να σας γράψω τις γραμμές τούτες.
- Γενικά, στο ΚΤΕΛ προτιμάμε θέσεις μπροστά. Σήμερα όμως, 23 του μήνα, όλοι φεύγουν από Θεσσαλονίκη για Χριστούγεννα. Το λεωφορείο είναι γεμάτο, οπότε αναγκαστικά πήραμε τις θέσεις 27, 28. Δεν μας αρέσει να καθόμαστε τόσο πίσω, αλλά τουλάχιστον έχουμε λίγο περισσότερο χώρο: μπροστά από τις θέσεις μας έχει κάτι σαν τραπεζάκι και μετά είναι η πόρτα, οπότε το να βολέψω κάπως το laptop και ν' αρχίσω να γράφω δεν στάθηκε αδύνατο.
- Ένα καλό που έχει το ΚΤΕΛ είναι οι ευκαιρίες που σου δίνει για ν' ακούς μουσική που υπό φυσιολογικές συνθήκες δεν έχεις την ευκαιρία ν' ακούς -- ή τουλάχιστον έτσι συμβαίνει με την περίπτωσή μου.
- Να, ακριβώς τώρα έχει Βασίλη Καρρά: Όσα κομμάτια κι αν μπορέσεις να ενώσεις, δεν θα σου φτάσουν μια στιγμή για να με νοιώσεις, στα είπα όοολααα κ.λπ. κ.λπ.
- Πριν είχε την κυρία Πάολα και πιο πριν πάλι Καρρά, με αυτό το θεϊκό εγώ καμάρα, κι εσύ πολυτεχνείοοοοο (τον τίτλο δεν τον θυμάμαι).

/var/log/messages

- Κάθε φορά που ακούω Καρρά, δεν μπορώ παρά να αναρωτηθώ για την ηλικία του. Καλά να είναι, απλά το αναφέρω γιατί είναι από εκείνους τους ανθρώπους οι οποίοι, όσο κι αν περνούν τα χρόνια, εμένα μου φαίνεται πως δεν αλλάζουν.
- Σας έχει συμβεί ποτέ αυτό; Να συνειδητοποιείτε ότι κάποιοι άνθρωποι είναι αναλλοίωτοι στο χρόνο; Εντάξει, είναι λογικό να έχουμε αυτή την εντύπωση για όσους είναι κοντά μας και τους βλέπουμε καθημερινά, αλλά μερικές φορές συμβαίνει και με άλλους, τους οποίους δεν έχουμε συναντήσει ποτέ. Για εμένα ο Καρράς είναι ένα παράδειγμα, η Κανέλλη ένα άλλο.
- Τέλος πάντων, δεν είναι μόνο αυτές οι σκέψεις που μ' απασχολούν αυτή τη στιγμή. Εδώ και μερικές ώρες σκέφτομαι τον καημένο τον virtualization host που έφτιαξα προσφάτως, ο οποίος έχει μείνει μόνος του στη Θεσσαλονίκη, δίπλα στο pfSense box. Δεν πρόκειται να πάθει κάτι το μηχάνημα. Μ' ανησυχεί όμως η σκέψη της διακοπής της πρόσβασης -- κι αναφέρομαι στη δική μου την πρόσβαση. Σήμερα το μεσημέρι βεβαιώθηκα ότι ο OpenVPN server στο pfSense box λειτουργεί σωστά, ώστε να έχω έναν τρόπο να φτάνω στο τοπικό δίκτυο πίσω του, άρα και στον virtualization host.
- Μη νομίζετε ότι έχω κάποια μεγάλη ανάγκη τα VMs του εν λόγω host, χριστουγεννιάτικα. Ίσως όμως χρειαστεί να συνδεθώ για να τσεκάρω κάτι ή για να βεβαιωθώ ότι κάτι άλλο δουλεύει όπως προβλέπεται. Ξέρετε κάτι; Δεν θα είχα την ανάγκη γι' αυτούς τους ελέγχους, αν είχα βάλει τις τελικές πινελιές σε ένα μίνι αφιέρωμα που ετοιμάζω για το τεύχος 049.
- Το μίνι αφιέρωμα αφορά στο virtulazion με το KVM και το openSUSE, μόνο που για άλλη μια φορά αποδείχθη ότι *και* μίνι δεν είναι *και* τον ατελείωτο έχει.
- Κλασικά.
- Κάτι που με αγχώνει μ' αυτόν τον πρόσφατο εκτροχιασμό είναι ο DTP guy του περιοδικού, ο οποίος με τη σειρά του αγχώνεται που έχει αυτή τη *μικρή* εκκρεμότητα με το PDF του νέου τεύχους. Είμαι επίσης σίγουρος ότι ανησυχεί κι ο κος Αρχισυντάκτης (TM). Αυτός όμως ανησυχεί σιωπηρά και δεν μιλάει. Είναι που για το τεύχος 049 δεν ετοίμασε κάποια άρθρο, λόγω έκτακτων υποχρεώσεων. Δυο-τρία τεύχη πριν ξεκίνησε μια σειρά άρθρων (όχι μίνι), γύρω από το πώς ακριβώς κατασκεύασε τον δικό του υπολογιστή -- κι εννοείται ότι δεν αναφέρομαι σε συναρμολόγηση PC.

Καταλάβατε τι έκανε; Μας έβαλε καλά καλά στην πρίζα με τα τέσσερα πρώτα άρθρα της σειράς, τώρα όμως μας βάζει στον πάγο. Τουλάχιστον υποσχέθηκε ότι θα επανέλθει από το τεύχος 050.

- Τώρα που είπα "πάγο", τι αισχρό αίσχος είν' αυτό με τον καιρό φέτος; Το μόνο παρήγορο --και μόλις προσπάθησα να κάνω air-quotes αλλά είμαι κάπως στριμωγμένος με το μπουφάν εδώ και φοβάμαι μη μου γλυστρήσει το laptop--, είναι ότι το κακό δεν έχει χτυπήσει μόνο την Ελλάδα, όπως άλλωστε συνηθίζει τα τελευταία χρόνια. Να, έβλεπα χθες λίγο την αγγλική εκδοχή του DW και είχε δελτίο καιρού: γύρω γύρω στη Γερμανία, παντού 12άρια βαθμών Κελσίου! Στο μεταξύ μου έλεγε κι ο Θείος Ακάκιος τα νέα του ανηψιού, ο οποίος ως γνωστόν έχει εγκατασταθεί, πρακτικά, στο Λονδίνο. Προς το παρόν, λέει, ο χειμώνας είναι ο πιο αφύσικα ζεστός για τα τελευταία χρόνια. Πάνε, λέει, να σπάσουν το ρεκόρ του '48.
- Έχει τώρα αρχίσει να στρίβει το ΚΤΕΛ, που εμποδίζεται από την πολλή κίνηση, για να μπει στο προαύλιο του σταθμού, στη Δράμα. Δεν ξέρω αν το λένε "προαύλιο". Μόλις τώρα το σκέφτηκα κι όσο σκέφτομαι ότι το σκέφτηκα, σκέφτομαι ότι μ' αρέσει αυτό που μόλις σκέφτηκα και θα το καθιερώσω να το λέω (αυτό που μόλις σκέφτηκα).
- Η κα Σύμβουλος Εκδόσεως (TM) κοιτάζει έξω από το παράθυρο τα φώτα της Ονειρούπολης, η οποία είναι δίπλα στο σταθμό. Κοιτάζω κι εγώ και το βλέμμα μου πέφτει σε μια ηλεκτρονική πινακίδα, που δείχνει τη θερμοκρασία.
- Οκτώ βαθμοί είναι ανεκτοί για την εποχή, και η γενική ατμόσφαιρα στη Δράμα ήδη δείχνει όμορφη και χριστουγεννιάτικη.
- Είμαι σίγουρος ότι είναι.
- Καλές γιορτές να έχουμε και να 'μαστε καλά, να φροντίζουμε την ονειρούπολή μας και να βοηθάμε τους ανθρώπους μας να φροντίζουν τη δική τους.



ονέλ, μέλ

Αγαπητοί μου,

Δεν θα σας κρατήσω σε αγωνία, δεν νομίζω πως έχει νόημα. Εγώ το έχω πάρει απόφαση. Τα πράγματα είναι απλά:

Δεν υπάρχει καμία μα καμία ελπίδα.

Ναι, ξέρω, πλησιάζουν --ακόμα και φέτος-- αι εορταί και θα περιμένατε φαντάζομαι να σας γράψω κάτι πιο αισιόδοξο, κάτι εορταστικό.

Όχι. Δεν μπορώ. Από όπου και να το κοιτάξω καταλήγω στο ίδιο συμπέρασμα.

Δεν υπάρχει καμία απολύτως ελπίδα.

Τι; Τι θα πει "σε τι αναφέρομαι"; Σε τίποτα δεν αναφέρομαι. Στα πάντα αναφέρομαι.

Ελλάδα, ας πούμε. Ξέρετε. Η Γαλανή μας Πατρίδα (TM).

Πότε είχαμε εκλογές; Χτες; Προχτές; Τέλος πάντων. Προ ημερών. Θυμάμαι, μη νομίζετε --κι ας με κακολογεί ο ανιψιός--, μια χαρά θυμάμαι.

Ο Κύριος Πρωθυπουργός (οθντκ). Είχε μόλις υπογράψει το δικό του μνημόνιο, ξέρετε ποιό, το "εκβιαστικό", το μετά το δημοψήφισμα, το με τις κλειστές τράπεζες. Το με χωρίς Γιάνη. Αυτό.

Τα φέρνει, λοιπόν, όλα στην Βουλή. Αμ' έπος, αμ' έργον.

Ψηφίζουν όλοι γιατί έχουν κατατρομάξει. Ποια διχαστικά δημοψηφίσματα και πρασινάλογα. Εκεί να δεις συναίνεση. Ο ορισμός της συναίνεσης.

Με δύο εξαιρέσεις: Το ΚΚΕ, από την μία, και οι χρυσαβγοί από την άλλη. Α, και η Zoe. Πυλώνες της αντιμνημονιακής αντίστασης. (BTW, αυτό δεν θα μας βγει σε καλό, να μου το θυμηθείτε.)

Τέλος πάντων, όλα τα χατήρια του κάνουν. Τον πιστεύουν. Ο Aleksis τους πείθει. Κάνουν την ανάγκη φιλοτιμία.

Ψηφίζεται λοιπόν το Μνημόνιο το $3^{ο}$ το Αριστερό, και τι κάνει ο τιτάνας της στρατηγικής; Εκλογές.

Εκλογές, το διανοείστε; Πρώτα ψηφάει τα μέτρα και μετά κάνει εκλογές. Αυτά έπρεπε να διδάσκονται στα πανεπιστήμια.

Δηλαδή τι; Κι αν έχανε;

Θα βγαίνανε μετά ξερω 'γω ποιοι, καμιά γαλαζοπράσινη ποταμίσια τσιπούρα, αναγκασμένη να υλοποιήσει το αριστερό μνημόνιο μιας και το είχε ψηφίσει, και θα είχε τον Aleksis στην Αντιπολίτευση να φωνάζει κατά του ΦΠΑ στα κουρεία και του ΕΝΦΙΑ στους αναπτήρες.

Ναι, καλά.

Πανικός. Βγαίνανε λοιπόν όλοι και τον παρακαλάγανε, τον Κύριο Πρωθυπουργό (οθντκ), "μην κάνεις εκλογές, άνθρωπε του θεού, την στήριξή μας την έχεις, μνημόνιο υπέγραψες, έλα, εντάξει, έλα θα τα βρούμε…"

Μπα... Χαμπάρι. Τίποτα. Εκλογές.

Αφού τον βλέπαμε με την μητέρα της Εξαδέλφης στον Ιντερνέ κι είχαμε

αρχίσει να αναρωτιόμαστε, βρε μπας και το έχει κανένα παιδικό τραύμα, με τις εκλογές και τις δημοκρατικές διαδικασίες, μήπως του βγαίνει έτσι, "υποσυνείδητα", και τον ξεπερνάει, μήπως δεν μπορεί να το ελέγξει. Να το βοηθήσει κάποιος το παιδί, να μιλήσει στην μάνα του, να τον ξεματιάσουν, κάτι να κάνουν τέλος πάντων.

Όχι. Αυτός θέλει εκλογές.

Ξανανικάει λοιπόν. Ο Κύριος Πρωθυπουργός (οθντκ). Εκ νέου. Μπλαμπλαμπλά δημοκρατία, μπλαμπλαμπλά με εκλέξατε κ.λπ.

Άντε πάλι μια από τα ίδια.

Και τι κυβέρνηση, ε; Δεύτερη φορά αριστερή. Ρηξικέλευθη.Επαναστατική. Μεταμοντέρνα.

Τέλος πάντων, τα θυμόμαστε όλοι αυτά. Πόσες ώρες, μέρες, βδομάδες έχουν περάσει από τις εκλογές; Δέκα; Έντεκα; Δώδεκα; Τόσες. Όχι περισσότερες. Τόσες.

Μόλις που προλάβανε να εορτάσουν τη ναυμαχία της Σαλαμίνας, κι αρχίσανε να μιλάνε ξανά για τα "προαπαιτούμενα". Και για την ανάγκη συναίνεσης.

Μπλαμπλαμπλά νωπή εντολή. Οι κακοί οι ξένοι. Τα προαπαιτούμενα. Μπλαμπλαμπλά δημοκρατία. Η δόση. Το ασφαλιστικό. Η πραγματική οικονομία. Οι ξένοι. Μπλαμπλαμπλά οι κακοί οι ξένοι.

Προαπαιτούμενα.

Λέξη κλειδί.

Προαπαιτώ proapetó -ούμαι (συνήθ. παθ.) : απαιτώ, αξιώνω, ζητώ κτ. εκ των προτέρων, προκαταβολικά (ως όρο ή προϋπόθεση): Για τη χορήγηση συναλλάγματος σε σπουδαστές προαπαιτείται η εγγραφή τους σε σχολή του εξωτερικού. Έγιναν όλες οι προαπαιτούμενες ενέργειες, ώστε να προχωρήσει η υπόθεση. // (μππ. ως ουσ.) τα προαπαιτούμενα, οι προϋποθέσεις, οι όροι. λόγ. ελνστ. προαπαιτω̃

Καμιά φορά μετανιώνω που το 'χω βάλει τάμα να σας γράφω με την γραφομηχανή, γιατί η γραφομηχανή δεν έχει κόπυ πέιστ. Δεν έχει, τι να κάνουμε. Το ως άνω το πληκτρολόγησα.

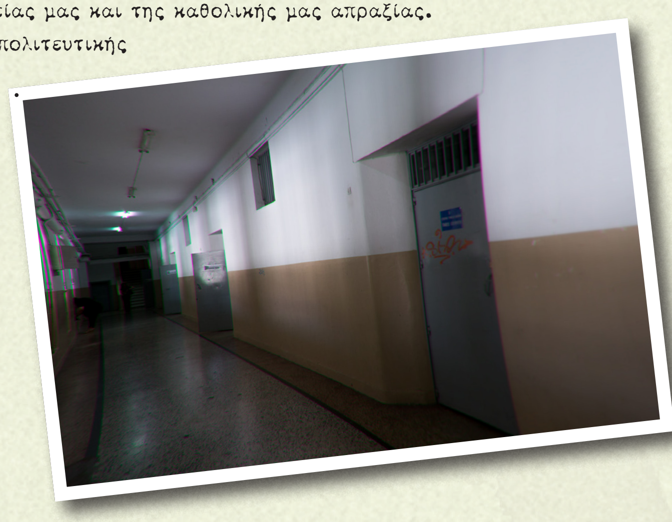
Θα το ήθελα, όμως, να έχει. Για κάτι μέρες σαν σήμερα. Γιατί αν είχε κόπυ πέιστ θα σας την είχα έτοιμη την επιστολή από χτες, και σήμερα θα είχα πάει σινεμά με την Μαιρούλα και την Εξαδέλφη. Έστω κι αν βρέχει.

Διότι, αγαπητοί μου, τα φετεινά προαπαιτούμενα, αυτά που έχουν κάνει τον Κύριο Πρωθυπουργό (οθντκ) να ζητάει συναίνεση και να κάνει μούτρα που δεν του την δίνουν, είναι ακριβώς τα ίδια, μα _ακριβώς_ τα ίδια με εκείνα που προαπαιτούνταν και προ πενταετίας. Το μόνο που έχει αλλάξει είναι οι ημερομηνίες (add 5 years).

Κόπυ πέιστ σας λέω. Αφού μου έρχεται ν' αφήσω τη γραφομηχανή και να πιάσω τον φορητό τη εξαδέλφης για να το βρω να σας το δείξω. Ψάξτε το.

Τα σημερινά προαπαιτούμενα λοιπόν είναι ίδια με τα προαπαιτούμενα του 2010. Το σημερινό μνημόνιο είναι ίδιο με του 2010, με ενσωματωμένη όλη την επιδείνωση (στο μεταξύ) κάθε μεγέθους της οικονομίας λόγω της βλακείας μας και της καθολικής μας απραξίας.

Και φυσικά λόγω της ώριμης αντιπολιτευτικής κριτικής του Aleksis και των φίλων του από την κάτω πλατεία.



ΟΚ, εντάξει. Θα μου πείτε, τι με έπιασε στα καλά του καθουμένου, τώρα το κατάλαβα ότι δεν έχει γίνει τίποτα -- κι ούτε πρόκειται ποτέ να γίνει;

Πραγματικά κι εγώ αναρωτιέμαι, αγαπητοί μου. Πηγαίνω κάθε λίγο στο μπάνιο, με κοιτάζω στον καθρέφτη και με ρωτάω. Περίμενα, ειλικρινά, πως θα είχε γίνει κάτι; Πως θα είχε κάποιος κάνει κάτι; Καλά πού ζω; Κάποιος, ποιος; Ο Aleksis;

συνέχεια

Αφού αυτός έβγαινε και μας υποσχόταν πως θα σκίσει, θα διώξει, θα απελευθερώσει, θα χορέψει, και δεν ξέρω τι άλλο. Μετά θα ξημέρωνε μια καινούργια μέρα.

Κι εμείς τον π ι σ τ ε ύ α μ ε!

Ναι, βεβαια, καινούργια μέρα ξημέρωσε, δε λέω. Και σήμερα το πρωί, καινούργια ήταν η μέρα.

Και τώρα είμαστε εδώ που είμαστε.

Από την μία έχεις τον Κύριο Πρωθυπουργό (οθντκ). Και από την άλλη έχεις την αντιπολίτευση. Μόλις βγήκανε από την σύσκεψη με τον Πρόεδρο της Δ. Σκυθρωποί. Δύσπιστοι.

Η αντιπολίτευση, ναι. Το δημοκρατικό τόξο. Η ευρωπαϊκή πορεία. Η ελπίδα του έθνους. Η πράσινη ελπίδα. Η γαλάζια.

Άνθρωποι με πείρα. Εχουν μάθει από τα λάθη του παρελθόντος. Κοιτάνε μπροστά. Εχουν όρεξη για δουλειά. Εχουν ιδέες. Ετοιμοι να κυβερνήσουν.

Ναι καλά, πάω για καφέ και φωνάξτε με όταν βγει το φαγητό.

Ας καταφέρουν πρώτα να εκλέξουν νέο αρχηγό, κι ας έρθουν μετά να κυβερνήσουν.

Αλλά ξέρω, ναι, είναι άνθρωποι της δουλειάς και του ιδρώτα. Με την τεχνολογία δεν τα πηγαίνανε ποτέ και τόσο καλά. Δεν πειράζει το φιάσκο. Καλή διάθεση να έχουμε κι όλα θα γίνουν.

Αγαπητοί μου,

Το βλέπετε τώρα αυτό που σας λέω;

Δεν υπάρχει ελπίδα. Καμία.

Και δεν υπάρχει, όχι γιατί οι κυβερνώντες είναι άχρηστοι. (Που είναι, δηλαδή, αλλά δεν είναι αυτό το θέμα.)

Ελπίδα δεν υπάρχει γιατί ακόμα και σήμερα, μετά από τα πέντε αυτά (σε λίγο έξι) χρόνια πρωτοφανών χαστουκιών και ταπείνωσης, συνεχίζουμε, ως κοινωνία, να πιστεύουμε πως κάπως θα γίνει, μαγικά, και όλα θα γίνουν ξανά όπως ήταν τα παλιά καλά χρόνια. Χωρίς να χρειαστεί να κάνουμε τίποτα. Ο Aleksis μας. Η αυτός που θα έρθει μετά τον Aleksis. Ο Κλούβιος και η Σουβλίτσα. Η Zoe. Τα Φουσκωτά Παληκάρια.

Θα έχουμε λεφτά, θα έχουμε μισθούς, θα κλέβουμε το κράτος, θα κλέβουμε ο ένας τον άλλο, θα παίρνουμε και καμιά επιδότηση από τους κουτόφραγκους, και θα την περνάμε ζάχαρη.

Είναι θέμα απόφασης. Άμα ο Ελληνας θέλει, όλα τα καταφέρνει.

Το μέλλον φαντάζει λαμπρό. Οι πρόσφυγες δεν θα έρχονται πλέον σε μας, οι Τούρκοι θα μας σέβονται, τα Σκόπια θα έχουν αλλάξει όνομα, οι Ισλαμιστές θα μας φοβούνται γιατί έτσι γράφει το Κοράνι, οι Αμερικανοί θα μας χρειάζονται γιατί είμαστε σε στρατηγικό γεωπολιτικό σημείο, οι Ρώσοι θα μας προστατεύουν γιατί μας ενώνει η Ορθόδοξη Πίστις, οι Γερμανοί θα μας έχουν δώσει όλες τις αποζημιώσεις που μας χρωστάνε, οπότε θα έχουμε αποπληρώσει το χρέος. Για να μην τα πολυλογώ, όλη η Οικουμένη θα έχει αναγνωρίσει τη μοναδικότητά μας, καθώς και αυτήν της γλώσσας μας που, όπως έχει πει και ο Μπιλ Γκέιτς, είναι η γλώσσα της πληροφορικής και της νέας γενιάς των εξελιγμένων υπολογιστών, διότι μόνο σ' αυτήν δεν υπάρχουν όρια.

Εμ τι νομίζατε;

Μπρίκια κολλάγαμε τόσο καιρό;

Σας ασπάζομαι,

Θείος Ακάκιος



Κάρτα e-coin, που δέχεται Bitcoins: Δουλεύει όπως όλες οι κανονικές κάρτες Debit, παντού στον κόσμο και για online αγορές.

Αποκτήστε τη δική σας με κλικ εδώ

και κερδίστε αυτομάτως

25% έκπτωση

κατά την παραγγελία της κάρτας.

Skill: Beginner
Tags: openSUSE, YaST, KVM, virtualization

Προσωπικό cloud με το openSUSE

[μέρος 1/2]

Έχετε ποτέ αναρωτηθεί τι εννοεί κάποιος που λέει ότι διαθέτει server ή/και storage στο cloud; Μην προσπαθήσετε να δώσετε μια επεξηγηματική ή έστω ικανοποιητικά γενική απάντηση. Πολύ απλά, ο φίλος μας εννοεί ότι χρησιμοποιεί τον υπολογιστή και τα μέσα αποθήκευσης Κάποιου Άλλου (TM) – κι ας μην το συνειδητοποιεί. Αν είσαστε από εκείνους που *δεν* σνομπάρουν τα οφέλη του cloud αλλά την ίδια στιγμή η ιδέα του να χρησιμοποιείτε ξένους πόρους δεν σας πολυαρέσει, αυτό το μίνι αφιέρωμα είναι για εσάς.

του Χρήστου Βαρελά

Ευθύς εξαρχής ξεκαθαρίζουμε ότι είμαστε φανατικοί οπαδοί του cloud. Για το περιοδικό κι όχι μόνο χρησιμοποιούμε εικονικούς servers, χώρους αποθήκευσης και υπηρεσίες λογισμικού που κατοικούν Εκεί Έξω (TM), στο cloud. Την ίδια στιγμή όμως μας αρέσει –και μας βολεύει– να έχουμε κι ένα μίνι, προσωπικό cloud, το οποίο δεν βρίσκεται ψηλά στον ουρανό αλλά κάπου εδώ κοντά, στο τοπικό δίκτυο της Parabing Creations. Και για να γίνουμε λίγο πιο συγκεκριμένοι, μιλώντας για "προσωπικό cloud" έχουμε κατά νου ένα φυσικό μηχάνημα ικανό να φιλοξενεί δύο ή περισσότερους εικονικούς υπολογιστές, οι οποίοι προσφέρουν ένα πλήθος υπηρεσιών. Ποιες μπορεί να 'ναι αυτές οι υπηρεσίες; Παραθέτουμε μερικά μόνο παραδείγματα: name server, proxy cache, database server, file server, Tor relay/middlebox, media server, Dropbox node, OpenVPN server, web server κ.ο.κ.

Για τους πειραματισμούς κατά την προετοιμασία άρθρων, για ορισμένες βασικές υπηρεσίες που χρειαζόμαστε στο τοπικό δίκτυο, όπως επίσης και για καθαρή διασκέδαση, στο παρελθόν έχουμε αρκετές φορές διαμορφώσει ένα PC ώστε ν' αναλαμβάνει καθήκοντα virtualization host. Μετά από μια σειρά τυχαίων περιστατικών που συνέβησαν σχετικά πρόσφατα (https://colder.xyz/exploding-disks), εδώ και λίγες μέρες το εν λόγω PC τρέχει το openSUSE LEAP (https://www.opensuse.org) και για το virtualization βασίζεται στην τεχνολογία του KVM (http://www.linux-kvm.org).

Το openSUSE εξ ορισμού εγκαθίσταται με περιβάλλον γραφικών (π.χ., KDE ή GNOME). Αν ο χρήστης το επιθυμεί μπορεί να έχει το λειτουργικό σύστημα χωρίς GUI, δηλαδή ως "καθαρόαιμο" server OS. Άλλωστε τα KVM VMs δεν χρειάζονται τοπικό display, είναι προσβάσιμα μέσω δικτύου και φυσικά δεν απαιτούν περιβάλλον

γραφικών από πλευράς host OS. Το ίδιο ισχύει και για τις εργασίες της δημιουργίας και της μετέπειτα διαχείρισης των VMs: Όλες είναι δυνατόν να πραγματοποιούνται είτε από τη γραμμή εντολής είτε με τη βοήθεια του κατάλληλου graphical client, ο οποίος τρέχει σε άλλο μηχάνημα.

Στο σημείο αυτό κάποιος θα μπορούσε να εγείρει ένσταση για τη χρήση του openSUSE ως host OS — κι αν αναφωνούσε κάτι σαν "Objection, Your Honor!" θα ήταν το ίνδαλμά μας. Θα ερωτούσαμε, τότε, " On what grounds?", και μάλλον θα μας απαντούσε με ένα ελαφρώς ειρωνικό "Relevance?". Το ερώτημα εδώ είναι γιατί να καταφύγουμε στο openSUSE με GUI, αντί σ' ένα περισσότερο server-oriented λειτουργικό, όπως, π.χ., είναι το Ubuntu Server LTS. Κι αν σώνει και καλά θέλαμε κάποιου είδους GUI από πλευράς host OS, θα μπορούσαμε να στραφούμε στο εξειδικευμένο Proxmox VE (http://deltahacker.gr/deltacast-s01e08), το οποίο μεταξύ άλλων παρέχει κι ένα εύχρηστο web panel. Η ένσταση λοιπόν είναι 101% έγκυρη. Μάλιστα πριν το openSUSE, από το ίδιο PC είχαν περάσει τα Ubuntu Server και Proxmox VE. Ο λόγος που αυτή τη φορά επιλέξαμε το openSUSE, ήταν γιατί συνειδητοποιήσαμε ότι συχνά θα θέλουμε να χρησιμοποιούμε το μηχάνημα κι ως σύστημα desktop. Η αντίστοιχη εκδοχή του Ubuntu είναι μια χαρά γ' αυτό το σκοπό, επειδή όμως το openSUSE έχει μια ξεχωριστή θέση στην καρδιά μας και προσφάτως κυκλοφόρησε και η νέα έκδοση (42.1 LEAP), αποφασίσαμε τελικά να πάμε μ' αυτό.

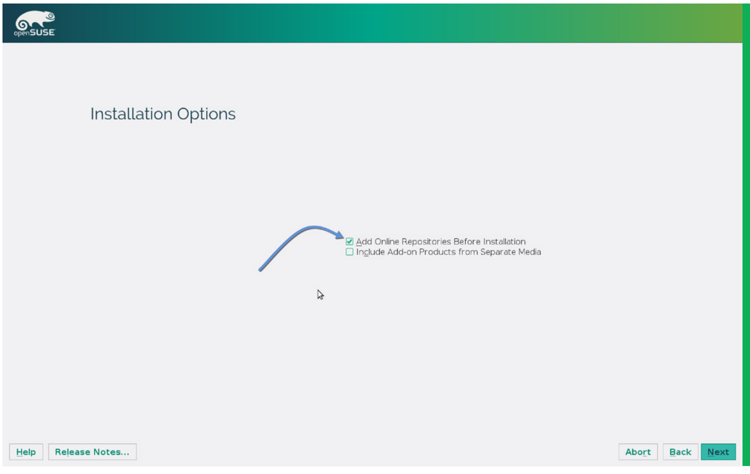
Στη συνέχεια βλέπουμε τη διαδικασία εγκατάστασης του openSUSE LEAP κι αμέσως μετά παραθέτουμε τις βασικές ρυθμίσεις που αξίζει να γίνουν στο λειτουργικό. Αν μας ακολουθήσετε, προς το τέλος του άρθρου θα έχετε ένα πλήρες σύστημα desktop για καθημερινή χρήση, το οποίο όμως έχει να προσφέρει πολλά περισσότερα απ' όσα γίνονται άμεσα αντιληπτά. Στο δεύτερο και τελευταίο άρθρο της μίνι σειράς, που αρχίζει από τη σελίδα 80, συνεχίζουμε με την εγκατάσταση της υποδομής virtualization και βλέπουμε πώς δημιουργούμε και διαχειριζόμαστε εικονικές μηχανές.

Προδιαγραφές συστήματος κι εγκατάσταση openSUSE

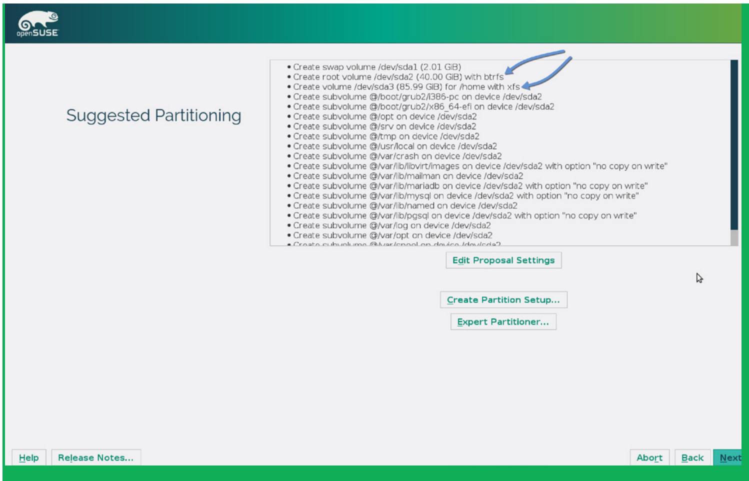
Το PC στο οποίο έγινε η εγκατάσταση διαθέτει έναν διπύρηνο επεξεργαστή Intel Core i3 με hyper-threading, επομένως σε λειτουργικό σύστημα κι εφαρμογές εμφανίζεται ως τετραπύρηνος. Η μνήμη RAM ανέρχεται στα 8GB κι αν η μητρική το επέτρεπε θα προσθέταμε άλλα οκτώ. Ωστόσο ακόμη και μ' αυτά τα σχετικά μέτρια χαρακτηριστικά, το μηχάνημα αποδίδει μια χαρά για τις ανάγκες μας: με συνετές ρυθμίσεις έχουμε καταφέρει να τρέχουμε άνετα έως και 6 VMs, ταυτόχρονα. Κατά τα άλλα, το PC διαθέτει μία μόνο κάρτα Gigabit Ethernet (μπροστά της έχει το pfSense box του τοπικού μας δικτύου) και τη στιγμή της εγκατάστασης διέθετε έναν μόνο δίσκο, χωρητικότητας 750GB. Λίγο μετά την εγκατάσταση του λειτουργικού προσθέσαμε κι έναν δεύτερο δίσκο, χωρητικότητας 1TB. Στο συγκεκριμένο δίσκο δώσαμε αποκλειστική κι απευθείας πρόσβαση σε ένα από τα VMs του openSUSE — αλλά επ' αυτού θα συζητήσουμε αργότερα.

Σημείωση. *Από τον virtualization host που φτιάχνουμε απουσιάζουν δυνατότητες όπως live migration, live backups, clustering κ.ά. Ακόμη και με ένα πιο εξειδικευμένο λειτουργικό σύστημα, όπως είναι το Proxmox VE ή το vSphere Hypervisor, για κάποιες από τις προαναφερθείσες δυνατότητες θα απαιτούταν εξειδικευμένο, ακριβό hardware (και περισσότερα από ένα boxes). Από τη στιγμή όμως που δεν έχουμε τόσο υψηλές απαιτήσεις, ένα τυπικό PC αρκεί. Κι όσο για το φλέγον θέμα του backup, χάρη στην πληθώρα των (φθηνών) προτάσεων online storage, ο κίνδυνος να χάσουμε κρίσιμα δεδομένα ελαχιστοποιείται.*

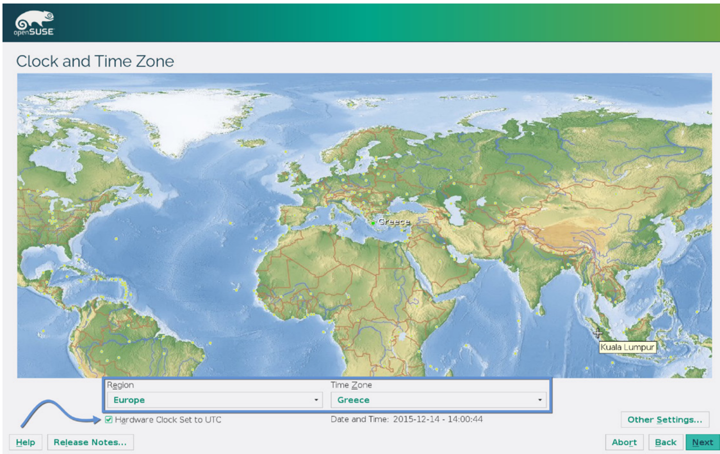
Γενικά, η εγκατάσταση του openSUSE δεν παρουσιάζει κάποια ιδιαιτερότητα. Για μερικά σημεία που αξίζουν της προσοχής μας, δείτε τα screenshots που ακολουθούν και διαβάστε τις αντίστοιχες περιγραφές.



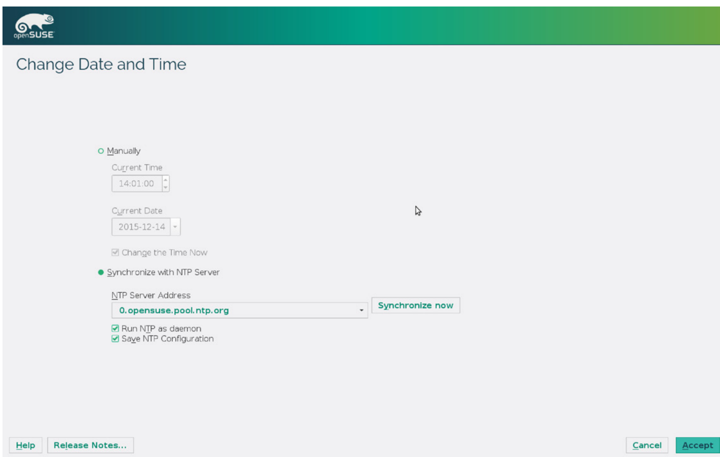
Η προσθήκη εφαρμογών κι εργαλείων, η ανανέωσή τους αλλά και οι αναβαθμίσεις του openSUSE, είναι εργασίες που θέλουμε να γίνονται από online repositories κι όχι από κάποιο φυσικό μέσο όπως, π.χ., το DVD ή το USB της εγκατάστασης. Τα online repositories μπορούμε βεβαίως να τα ενεργοποιήσουμε αργότερα, μετά την εγκατάσταση του λειτουργικού – ή ακόμη και σ' αυτό το πρώιμο στάδιο της διαδικασίας.



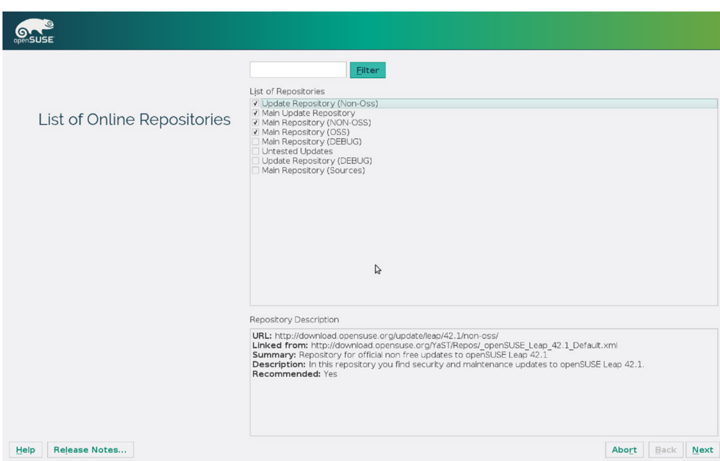
Ο installer του openSUSE προτείνει μια διευθέτηση του πρώτου δίσκου σε διαμερίσματα (partitions), τα οποία διαμορφώνονται κατά το σύστημα αρχείων XFS (το /home) αλλά και κατά το BtrFS (διάφορα subvolumes κάτω από το /). Το BtrFS δείχνει να είναι το μέλλον για τα συστήματα αρχείων του Linux και κατά πολλούς αποτελεί το αντίπαλο δέος του ZFS. Προς το παρόν δεν κρίνεται ως αρκετά αξιόπιστο ώστε να 'ναι η προεπιλογή στις διανομές Linux, αλλά βελτιώνεται διαρκώς. Για το PC μας, πάντως, πραγματικά δεν υπάρχει λόγος ν' αγχωνόμαστε και με χαρά αποδεχόμαστε την πρόταση του installer. (Σημείωση: Το screenshot προέρχεται από VMware VM κι όχι από το ίδιο το μηχάνημα της εγκατάστασης.)



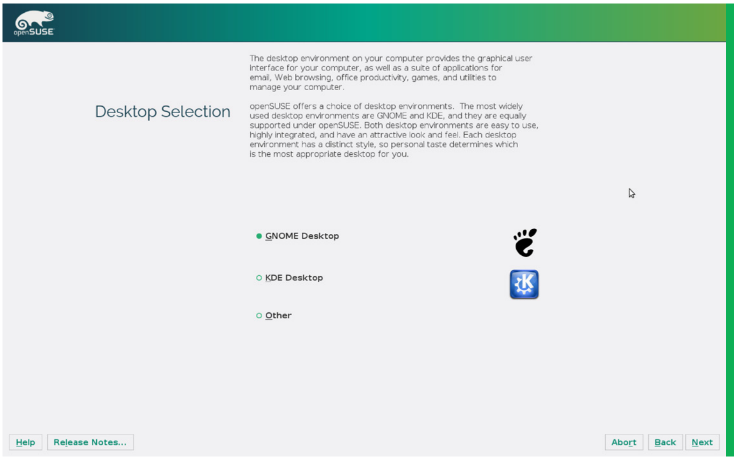
Επιλογή ζώνης ώρας. Μην ξεχάσετε να τσεκάρετε το Hardware Clock Set to UTC. Μόνος λόγος για να μην το κάνετε είναι αν στο PC υπάρχουν ήδη τα Windows και θέλετε dual boot με το openSUSE.



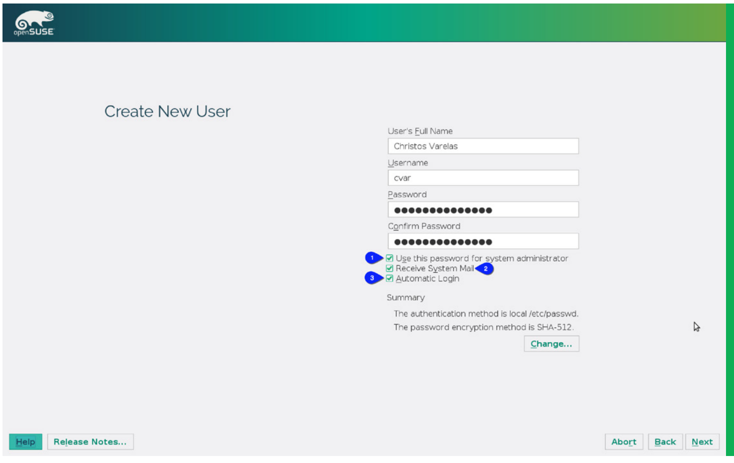
Στην προηγούμενη οθόνη, κάντε ένα κλικ στο κουμπί Other Settings και βεβαιωθείτε ότι το ρολόι του συστήματος συγχρονίζεται όχι χειροκίνητα (manually) αλλά αυτόματα, από NTP server.



*Επιλογή των online repositories που επιθυμούμε να είναι ενεργά. Ουσιαστικά, αυτά που *δεν* θέλουμε είναι τα δύο DEBUG repositories, εκείνο με τα untested updates – καθώς κι αυτό με τα sources.*



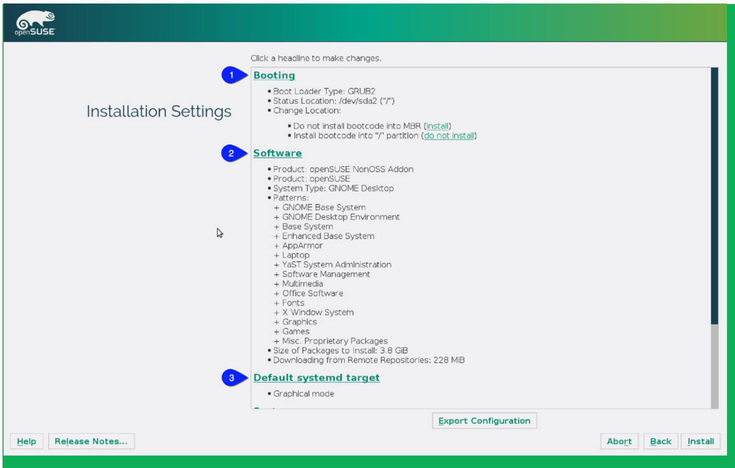
Επιλογή περιβάλλοντος γραφικών για μετά την εγκατάσταση. Το πλέον δημοφιλές μεταξύ των φίλων του openSUSE είναι το KDE. Όχι τυχαία, αφού η διανομή πάντοτε το υποστήριζε άψογα. Το KDE όμως είναι κάπως βαρύ και μάλλον περιττό για τη χρήση που σκοπεύουμε να κάνουμε, οπότε επιλέγουμε το GNOME.



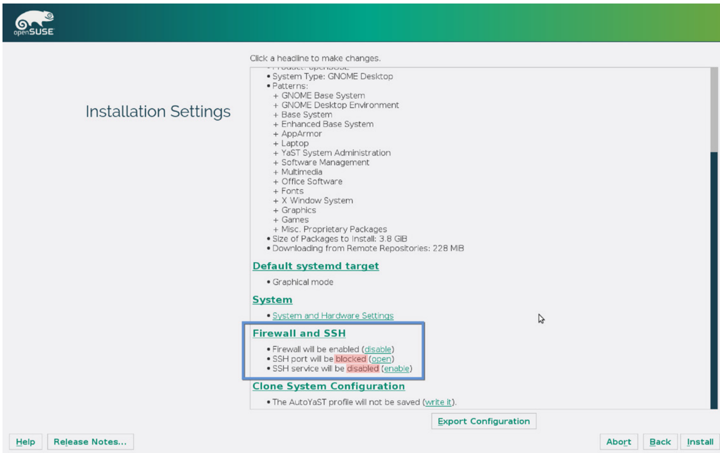
Οφείλουμε να δημιουργήσουμε τουλάχιστον έναν λογαριασμό απλού χρήστη. Χρειαζόμαστε μόνο έναν και φροντίζουμε ώστε:

- *να έχει δικαιώματα διαχείρισης συστήματος (1),*
- *να λαμβάνει το email του root (2),*
- *μετά την εκκίνηση του λειτουργικού να συνδεόμαστε αυτόματα στο λογαριασμό, χωρίς την πληκτρολόγηση του αντίστοιχου password (3).*

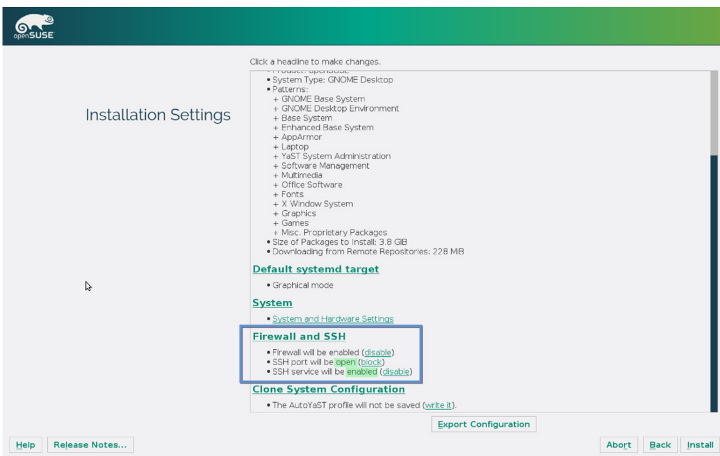
Οποιαδήποτε απ' αυτές τις επιλογές είναι δυνατόν ν' αλλάξει και μετά την εγκατάσταση.



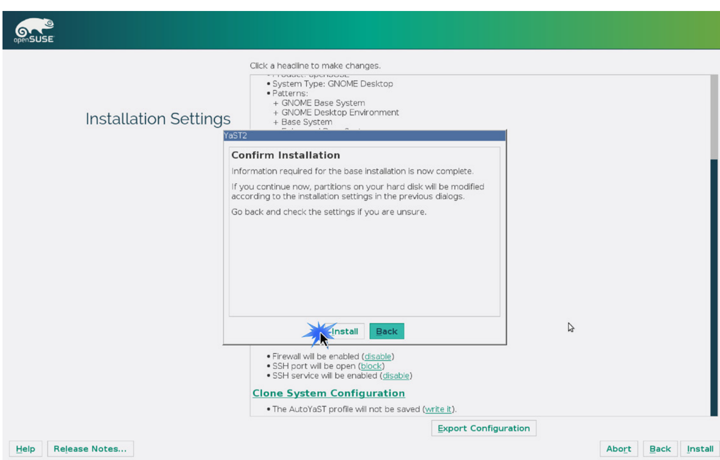
Ιδού όλες οι παράμετροι της εγκατάστασης. Πριν ξεκινήσει η διαδικασία έχουμε τη δυνατότητα να τροποποιήσουμε όσες παραμέτρους θέλουμε, ώστε μετά το πέρας της εγκατάστασης το σύστημα να έχει τις ιδιότητες και τη συμπεριφορά που εμείς επιθυμούμε. Μπορούμε, π.χ., να καθορίσουμε το χρόνο παραμονής του μενού του bootloader (1), να φροντίσουμε για την παρουσία συγκεκριμένων προγραμμάτων αμέσως μετά την εγκατάσταση (2), να κανονίσουμε ώστε μετά την εκκίνηση να μην ενεργοποιείται αυτόματα το περιβάλλον γραφικών (3) κ.ά. Δείτε στα δύο επόμενα screenshots δύο παραμέτρους που πάντα θέλουμε να τροποποιούμε.



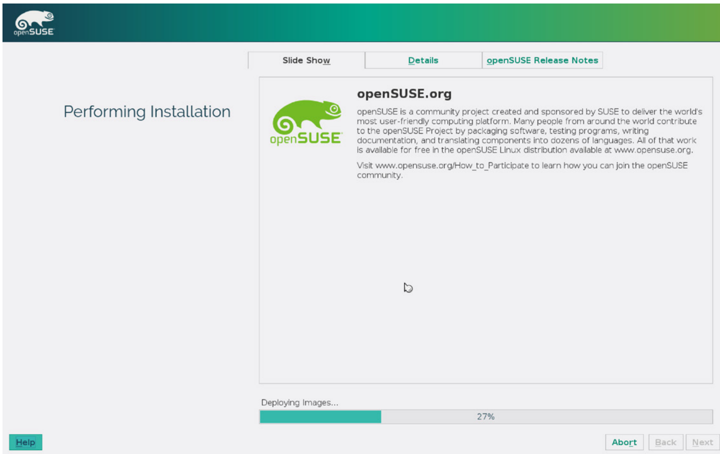
Το openSUSE είναι από τις λίγες διανομές Linux η οποία μετά την εγκατάσταση έχει το firewall ενεργοποιημένο. Όπως βλέπετε το port της υπηρεσίας SSH (για απομακρυσμένες, ασφαλείς συνδέσεις) είναι μπλοκαρισμένο, ενώ και η ίδια η υπηρεσία είναι ανενεργή.



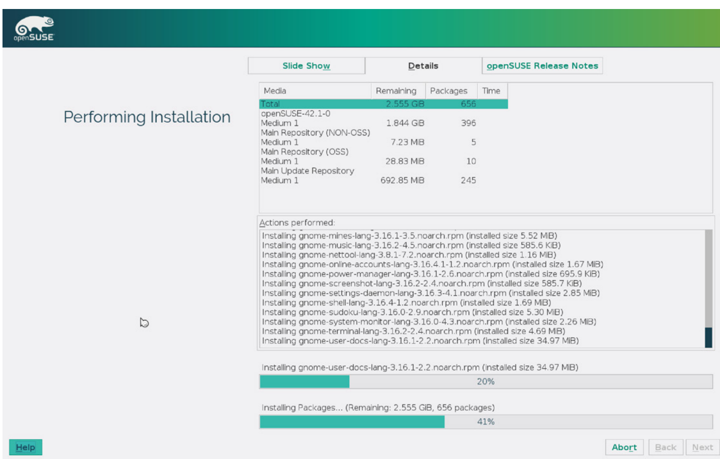
Στον virtualization host χρειαζόμαστε απομακρυσμένη πρόσβαση μέσω SSH, συνεπώς ανοίγουμε το port κι ενεργοποιούμε την υπηρεσία.



Αυτή η προειδοποίηση πριν την έναρξη της διαδικασίας εγκατάστασης αποτελεί την τελευταία μας ευκαιρία για αλλαγές. Εμείς είμαστε μια χαρά, οπότε απλά κάνουμε ένα κλικ στο κουμπάκι Install.



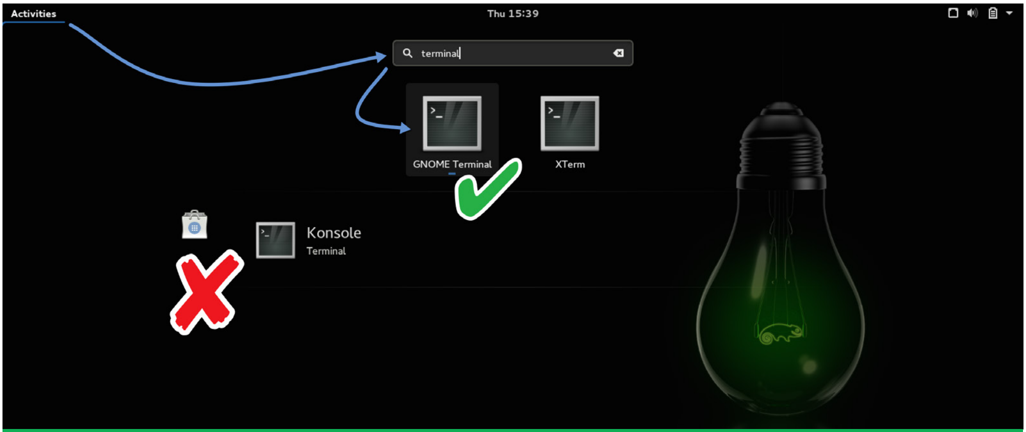
Από εδώ και πέρα δεν έχουμε κάτι να κάνουμε. Μετά από λίγα λεπτά η διαδικασία της εγκατάστασης θα έχει ολοκληρωθεί κι εμείς θα βρισκόμαστε συνδεδεμένοι στο λογαριασμό του χρήστη που προηγουμένως δημιουργήσαμε.



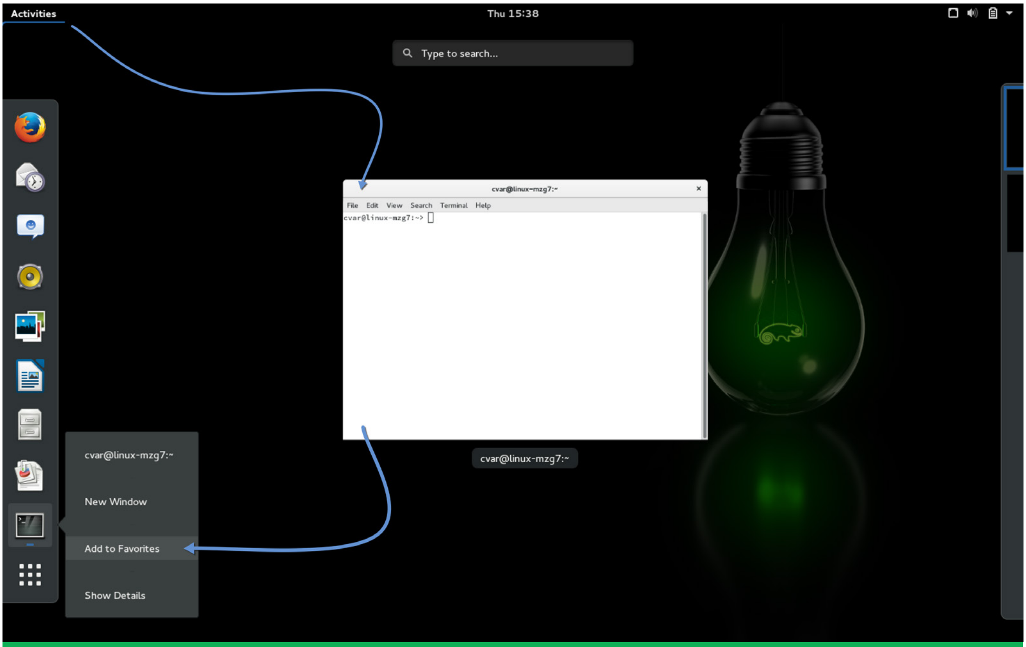
*Λεπτομέρειες και στατιστικά κατά την εγκατάσταση πακέτων. Όπως διεφάνη έως τώρα, σε σύγκριση με το Ubuntu το openSUSE αφήνει το χρήστη να βλέπει περισσότερα από την εσωτερική λογική και αρχιτεκτονική του συστήματος. Καθώς θα χρησιμοποιείτε το λειτουργικό, αυτή η αρχική σας υποψία θα μετατραπεί σε βεβαιότητα. Στοιχηματίζουμε ότι το openSUSE θα κερδίσει *και* εσάς.*

Βασικές ρυθμίσεις μετά την εγκατάσταση

Το desktop του GNOME είναι εξαιρετικά απλό και, για το γούστο μας αλλά και για τον προσανατολισμό του μηχανήματος, πολύ καλά κάνει και είναι εξαιρετικά απλό. Ούτως ή άλλως, την περισσότερη ώρα που θα καθόμαστε μπροστά από το συγκεκριμένο PC θα δουλεύουμε με ένα ή περισσότερα παράθυρα τερματικού και με τον λεγόμενο Virt-Manager (https://virt-manager.org). Ακριβώς γι' αυτό, ξεκινάμε φέρνοντας στο panel εφαρμογών ένα παράθυρο για το GNOME Terminal.



Με ένα κλικ στο Activities, πάνω αριστερά στο GNOME desktop, εμφανίζεται μια θυρίδα στην οποία πληκτρολογούμε το όνομα μιας οποιασδήποτε εφαρμογής. Πληκτρολογώντας "terminal" παίρνουμε δύο αποτελέσματα, τα οποία αντιστοιχούν σε δύο προεγκατεστημένες εφαρμογές τερματικού. Αυτή που μας ενδιαφέρει είναι η GNOME Terminal. Παρατηρήστε ότι στα αποτελέσματα πήραμε και το Konsole, που είναι το όνομα της αντίστοιχης εφαρμογής τερματικού για το περιβάλλον του KDE. Το Konsole δεν είναι εγκατεστημένο κι αν κάνουμε το λάθος να το εγκαταστήσουμε μαζί του θα έρθουν και 129 (περίπου) dependencies από τον κόσμο του KDE, εντελώς άχρηστα για το περιβάλλον του GNOME.



*Το GNOME Terminal τρέχει και, προκειμένου να έχουμε το αντίστοιχο εικονίδιο μόνιμα στο panel του GNOME, πατάμε στο Activities, κάνουμε δεξί κλικ στο εικονίδιο του GNOME Terminal πάνω στο panel και, τέλος, επιλέγουμε Add to Favorites. Ομοίως προσθέτουμε κι άλλα εικονίδια χρήσιμων ή/και συχνά χρησιμοποιούμενων εφαρμογών, όπως, π.χ., το YaST ή ο Virt-Manager (δεν τον έχουμε εγκαταστήσει ακόμα). Το ίδιο εύκολα απομακρύνουμε εικονίδια εφαρμογών που *δεν* χρησιμοποιούμε συχνά -- και τα εικονίδια του OpenOffice συνήθως φεύγουν πρώτα.*

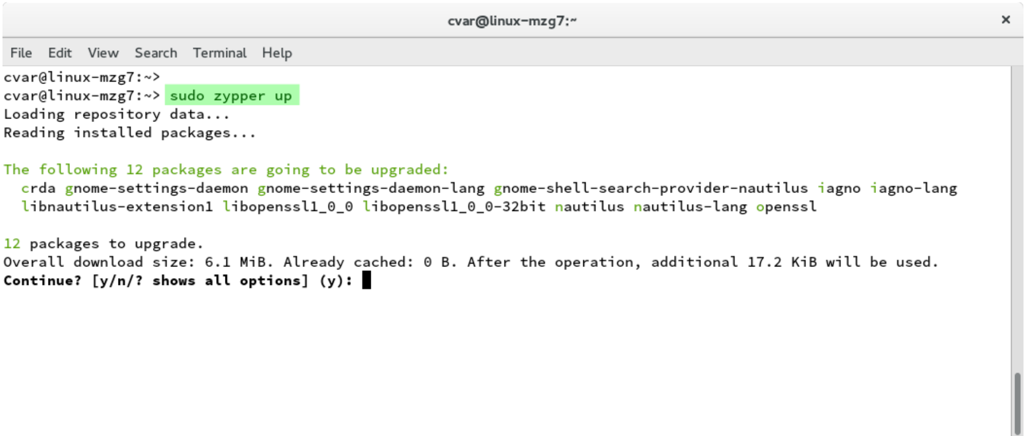
Από τη στιγμή που έχουμε το ωραιότατο τερματικό μας, η επόμενη εργασία που αξίζει να κάνουμε είναι να φρεσκάρουμε τα repositories πακέτων του openSUSE κι αμέσως μετά να εφαρμόσουμε τις όποιες διαθέσιμες αναβαθμίσεις. Αμφότερες οι εργασίες γίνονται και με τη βοήθεια του σχετικού module του YaST, εννοείται όμως ότι σαν το τερματικό δεν έχει.

```
cvar@linux-mzg7:~
File  Edit  View  Search  Terminal  Help
cvar@linux-mzg7:~>
cvar@linux-mzg7:~> sudo zypper ref
Repository 'Main Repository (NON-OSS)' is up to date.
Repository 'Update Repository (Non-Oss)' is up to date.
Repository 'Main Repository (OSS)' is up to date.
Repository 'Main Update Repository' is up to date.
Repository 'openSUSE-42.1-0' is up to date.
Repository 'openSUSE-Leap-42.1-Update' is up to date.
All repositories have been refreshed.
cvar@linux-mzg7:~>
```

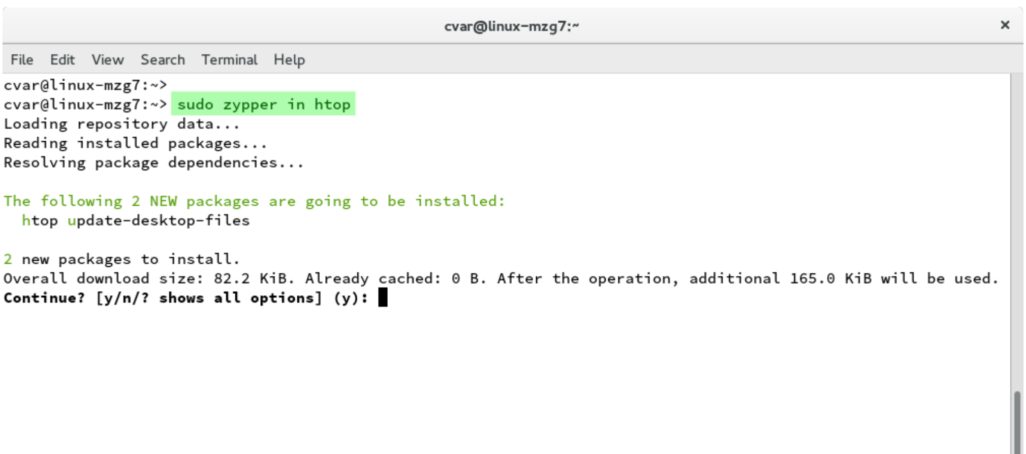
Για το φρεσκάρισμα των repositories εφαρμογών του openSUSE, πληκτρολογούμε απλά "sudo zypper ref" (χωρίς τα εισαγωγικά). Το "ref" αποτελεί συντόμευση του "refresh".

```
cvar@linux-mzg7:~
File  Edit  View  Search  Terminal  Help
cvar@linux-mzg7:~>
cvar@linux-mzg7:~> sudo zypper lu
Loading repository data...
Reading installed packages...
S | Repository             | Name                                   | Current Version | Available Version | Arch
--+------------------------+----------------------------------------+-----------------+-------------------+-------
v | Main Update Repository | crda                                   | 1.1.3-3.2       | 3.18-5.1          | x86_64
v | Main Update Repository | gnome-settings-daemon                  | 3.16.3-4.1      | 3.16.4-7.1        | x86_64
v | Main Update Repository | gnome-settings-daemon-lang             | 3.16.3-4.1      | 3.16.4-7.1        | noarch
v | Main Update Repository | gnome-shell-search-provider-nautilus   | 3.16.2-2.5      | 3.16.3-5.1        | x86_64
v | Main Update Repository | iagno                                  | 3.16.1-3.6      | 3.16.2-6.1        | x86_64
v | Main Update Repository | iagno-lang                             | 3.16.1-3.6      | 3.16.2-6.1        | noarch
v | Main Update Repository | libnautilus-extension1                 | 3.16.2-2.5      | 3.16.3-5.1        | x86_64
v | Main Update Repository | libopenssl1_0_0                        | 1.0.1i-6.1      | 1.0.1i-9.1        | x86_64
v | Main Update Repository | libopenssl1_0_0-32bit                  | 1.0.1i-6.1      | 1.0.1i-9.1        | x86_64
v | Main Update Repository | nautilus                               | 3.16.2-2.5      | 3.16.3-5.1        | x86_64
v | Main Update Repository | nautilus-lang                          | 3.16.2-2.5      | 3.16.3-5.1        | noarch
v | Main Update Repository | openssl                                | 1.0.1i-6.1      | 1.0.1i-9.1        | x86_64
cvar@linux-mzg7:~>
```

Μετά το φρεσκάρισμα των repositories, τις όποιες διαθέσιμες αναβαθμίσεις πακέτων τις βλέπουμε πληκτρολογώντας "sudo zypper lu". Το "lu" είναι συντόμευση του "list-updates".



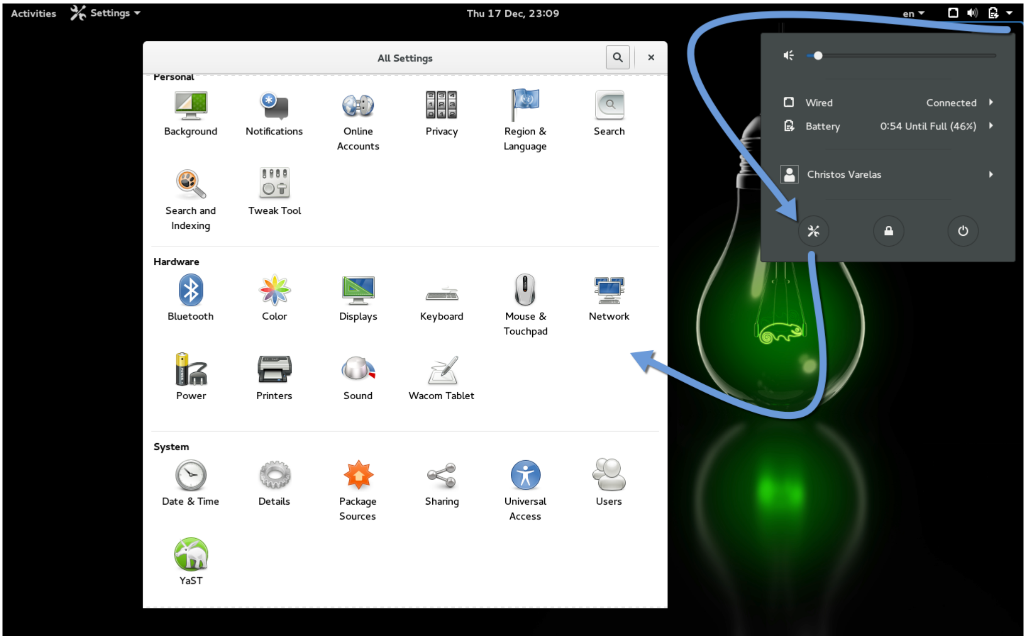
Η αναβάθμιση των πακέτων επιτυγχάνεται δίνοντας "sudo zypper up", όπου το "up" αποτελεί συντόμευση του "update".



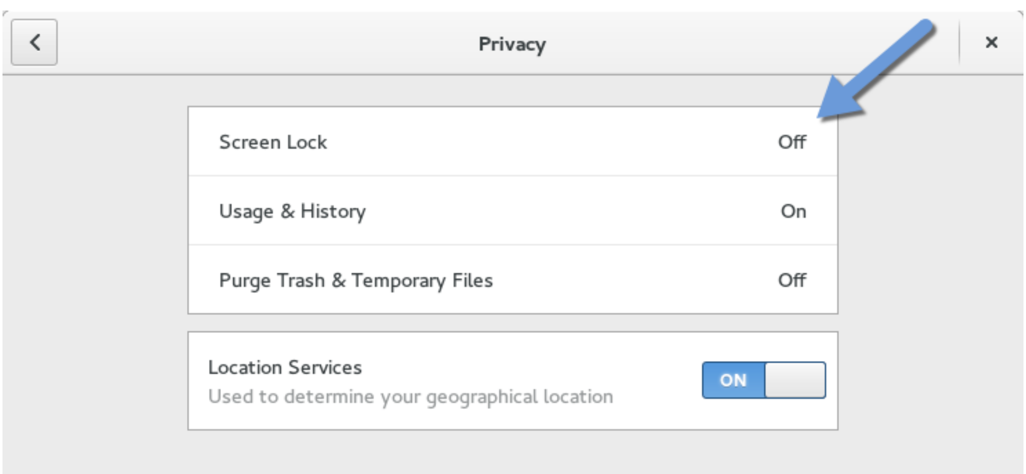
Και μετά τις αναβαθμίσεις ίσως θελήσουμε να εγκαταστήσουμε κάποια εργαλεία, χωρίς τα οποία δεν μπορούμε να κάνουμε. Να, εμείς π.χ. θέλουμε ανά πάσα στιγμή να έχουμε εύκαιρο το htop. Η εντολή που δίνουμε στο zypper για τις εγκαταστάσεις είναι η "in" (συντόμευση του "install").

Το openSUSE στα μέτρα μας

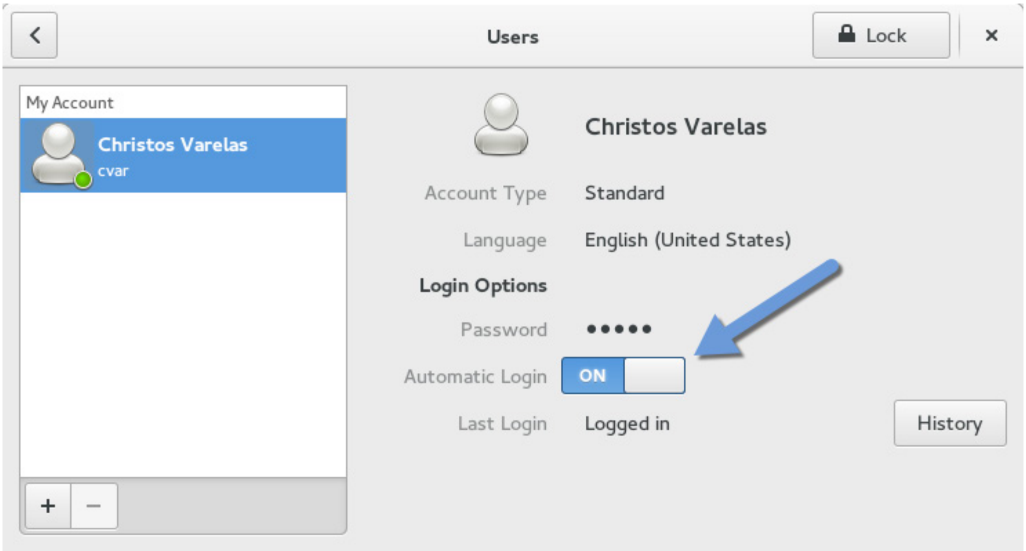
Εδώ που έχουμε φτάσει διαθέτουμε ένα σύγχρονο, σταθερό και πλήρως ενημερωμένο λειτουργικό σύστημα, ικανό να καλύπτει τις καθημερινές μας ανάγκες αλλά και πιο εξειδικευμένες, όπως, π.χ., να αποτελέσει έναν πανίσχυρο virtualization host για το τοπικό μας δίκτυο. Επ' αυτού έχουμε πολλά να πούμε και να δείξουμε στο άρθρο που ξεκινά από τη σελίδα 80. Προς το παρόν, προκειμένου ν' αποκτήσουμε μια καλύτερη αίσθηση του νέου μας λειτουργικού συστήματος, πιστεύουμε ότι αξίζει να δούμε και να επέμβουμε σε κάποιες ρυθμίσεις που αφορούν στο GNOME desktop — αλλά και στο ίδιο το σύστημα. Ξεκινάμε με το desktop.



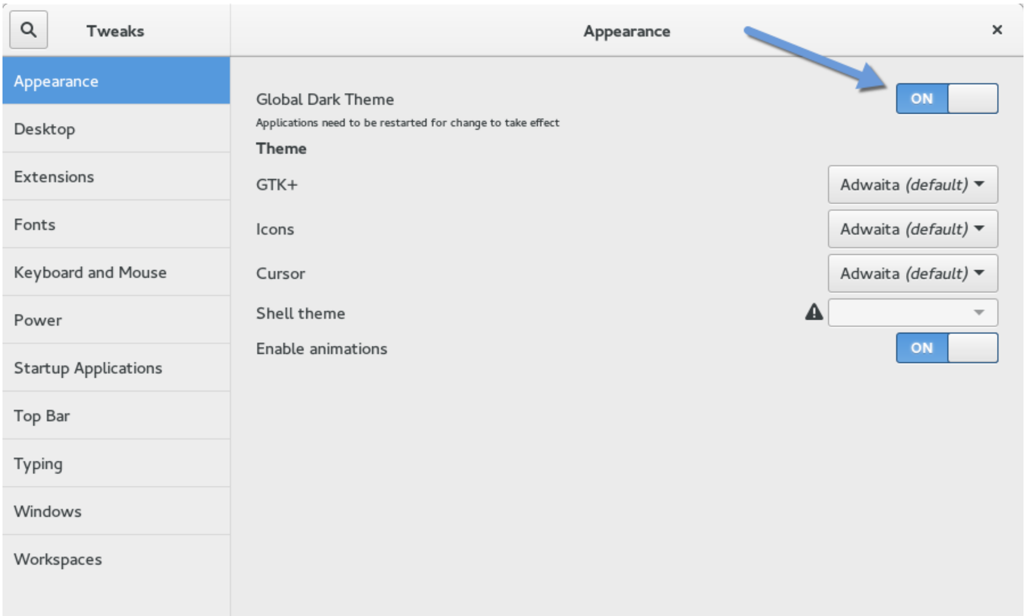
Θέλουμε τον πίνακα ελέγχου του GNOME κι ένας τρόπος για να τον έχουμε είναι με δύο μόλις κλικ, όπως φαίνεται στο στιγμιότυπο. Βλέπουμε ένα πλήθος εικονιδίων κατηγοριοποιημένα ανά είδος ρυθμίσεων (Personal, Hardware και System). Προτείνουμε να κάνετε κλικ σε όλα τα εικονίδια και να δείτε τις αντίστοιχες επιλογές με την ησυχία σας. Στα επόμενα στιγμιότυπα δείχνουμε μερικές από τις επεμβάσεις που μας αρέσει να κάνουμε.



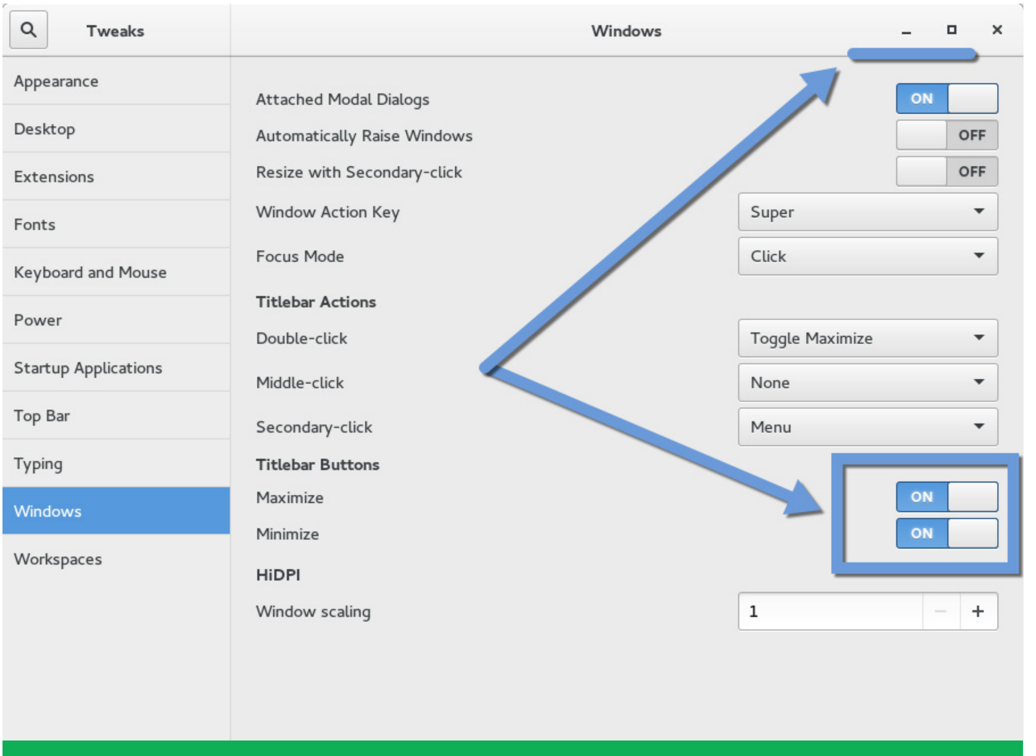
Εξ ορισμού, όταν είμαστε συνδεδεμένοι στο λογαριασμό του χρήστη μας αλλά δεν αλληλεπιδρούμε με το λειτουργικό, μετά από λίγο η οθόνη "κλειδώνει" και για ν' αποκτήσουμε ξανά πρόσβαση στο λογαριασμό χρειάζεται να πληκτρολογήσουμε το αντίστοιχο password. Από πλευράς ασφαλείας πρόκειται για καλή πρακτική. Το συγκεκριμένο PC όμως το χρησιμοποιούμε μόνον εμείς, οπότε το να συνειδητοποιούμε κάθε λίγο και λιγάκι ότι πρέπει να δώσουμε password είναι κάπως ενοχλητικό. Γι' αυτό, λοιπόν, θέτουμε Screen Lock = Off (εικονίδιο Privacy, κατηγορία Personal).



Κατά τη διάρκεια της εγκατάστασης του openSUSE, όταν δημιουργήσαμε το χρήστη μας φροντίσαμε ώστε μετά από κάθε boot του συστήματος να συνδεόμαστε αυτόματα στο λογαριασμό του. Όποτε θελήσουμε ν' αλλάξουμε τη συγκεκριμένη πολιτική ασφαλείας το κάνουμε από εδώ (εικονίδιο Users, κατηγορία System).



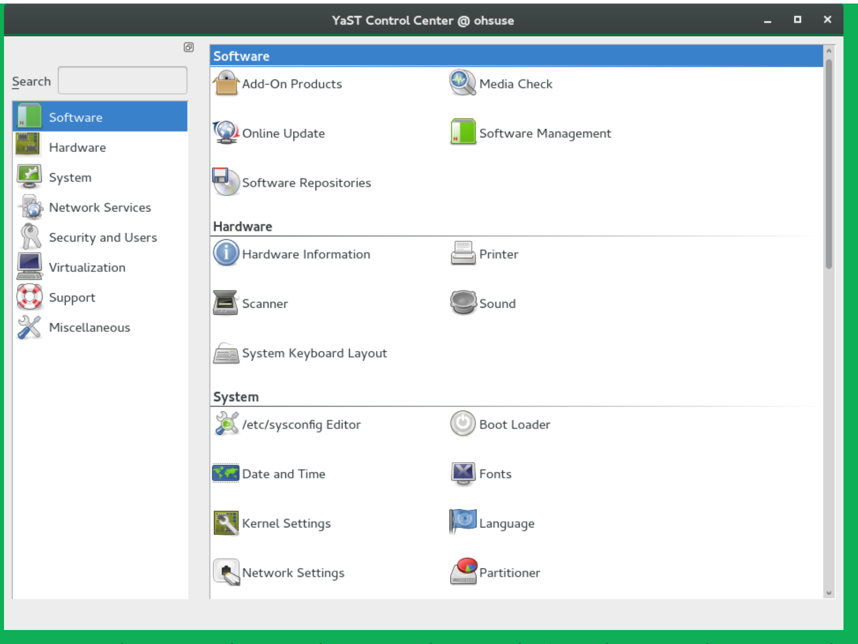
Στην κατηγορία Personal του πίνακα ελέγχου υπάρχει το εικονίδιο ονόματι Tweak Tool. Με κλικ πάνω του ανοίγει το παράθυρο Tweaks και μέσα απ' αυτό αποκτάμε πρόσβαση σε μια πληθώρα ρυθμίσεων που αφορούν στην εμφάνιση αλλά και στη συμπεριφορά του GNOME desktop. Στην πρώτη από πάνω κατηγορία του παραθύρου Tweaks, την Appearance, σ' εμάς αρέσει να ενεργοποιούμε το σκοτεινό theme (Global Dark Theme = On). Τα οπτικά αποτελέσματα του σκοτεινού theme γίνονται φανερά στα νέα παράθυρα που θα ανοίξουμε. Προτείνουμε να το δοκιμάσετε. Αν δεν σας αρέσει απλά θα έρθετε ξανά εδώ και θα θέσετε Global Dark Theme = Off.



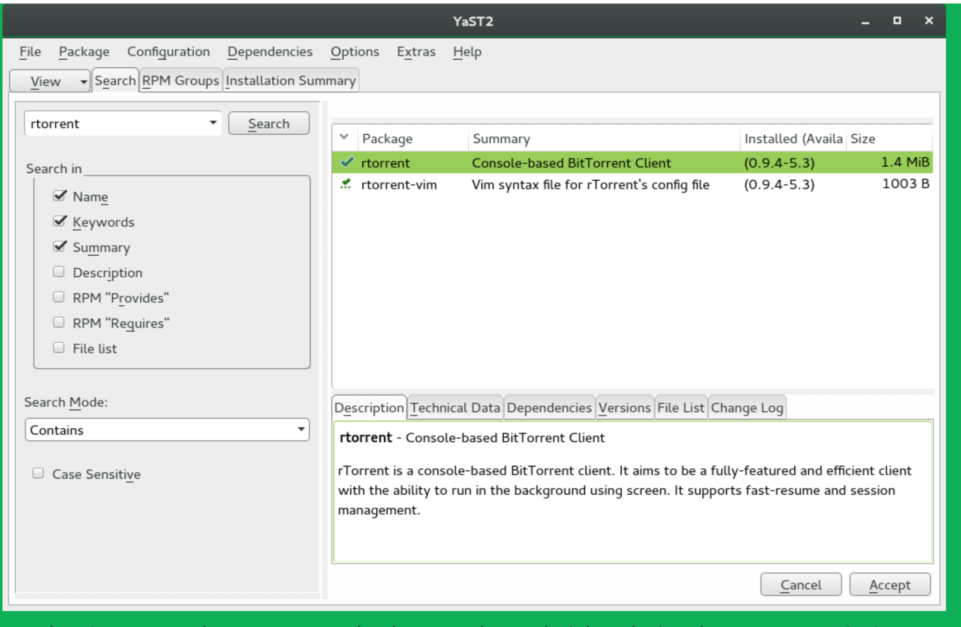
Τα κουμπιά της ελαχιστοποίησης και της μεγιστοποίησης των παραθύρων, εξ ορισμού είναι απενεργοποιημένα στο GNOME. Μπορούμε εύκολα να τα ενεργοποιήσουμε μέσα από το παράθυρο Tweaks – και συγκεκριμένα από την κατηγορία Windows.

Διαχείριση συστήματος με το YaST

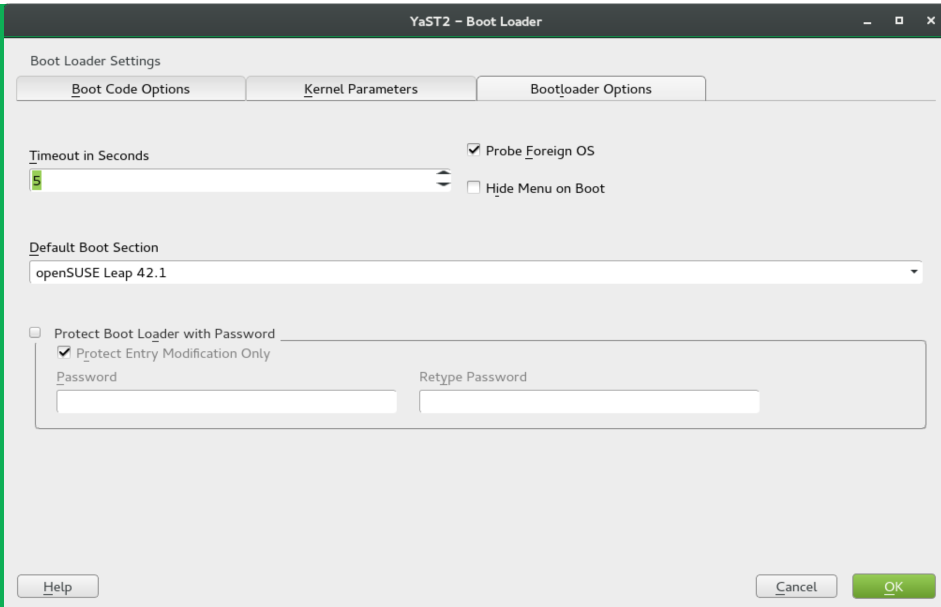
Το YaST (Yet another Setup Tool) είναι το μοναδικό ίσως πρόγραμμα που ανέκαθεν ξεχώριζε το openSUSE από άλλες διανομές Linux. Χωρίς καν να το συνειδητοποιήσουμε, το YaST το γνωρίσαμε ήδη από το στάδιο της εγκατάστασης του λειτουργικού. Αργότερα, μέσω των επιμέρους modules που απαρτίζουν την εφαρμογή, έχουμε δυνατότητα επέμβασης σε διάφορες όψεις του συστήματος που αφορούν στο hardware, στο software, στη δικτύωση, στην ασφάλεια κ.ά. Ένας τρόπος για να τρέξουμε το YaST είναι με κλικ στο σχετικό εικονίδιο του πίνακα ελέγχου (βλ. κατηγορία System). Στο δεύτερο άρθρο της μίνι σειράς μας θα ξεκινήσουμε με το YaST, ώστε να μετατρέψουμε το PC μας σε virtualization host. Προς το παρόν, δείτε μερικά από τα modules του προγράμματος σε δράση.



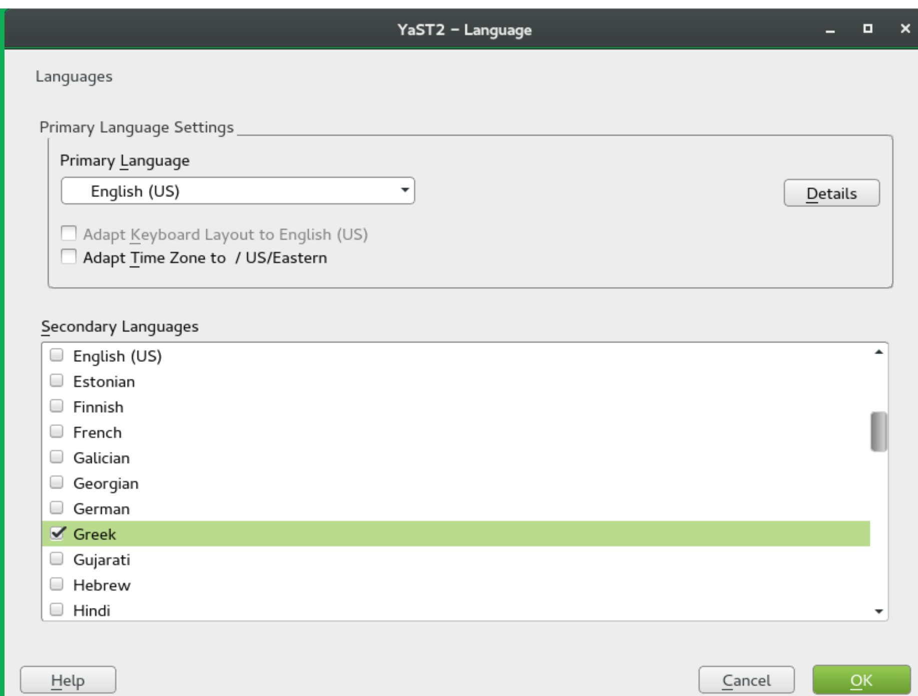
Τα modules του YaST είναι οργανωμένα σε οκτώ διαφορετικές κατηγορίες (βλ. στήλη αριστερά). Με την ησυχία σας, ενεργοποιήστε ένα ένα τα modules και δείτε τι δυνατότητες παρέμβασης/παραμετροποίησης προσφέρουν. Περιττό να πούμε πως αν δεν είστε βέβαιοι για κάποια ρύθμιση ή για τις επιπτώσεις που επιφέρει η τροποποίησή της, αφήστε την ως έχει.



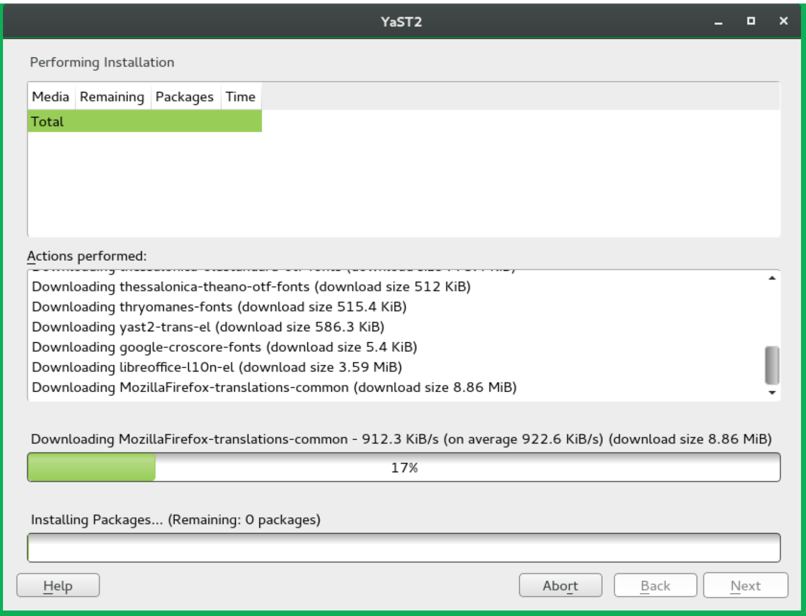
Αν δεν είστε fan της εγκατάστασης λογισμικού από τη γραμμή εντολών (λέμε τώρα), υπάρχει και το YaST (Software → Software Management). Στο στιγμιότυπο ετοιμαζόμαστε να εγκαταστήσουμε τον αγαπημένο μας BitTorrent client ονόματι rtorrent, ο οποίος, αϊρόνικλι ινάφ, λειτουργεί σε text console.



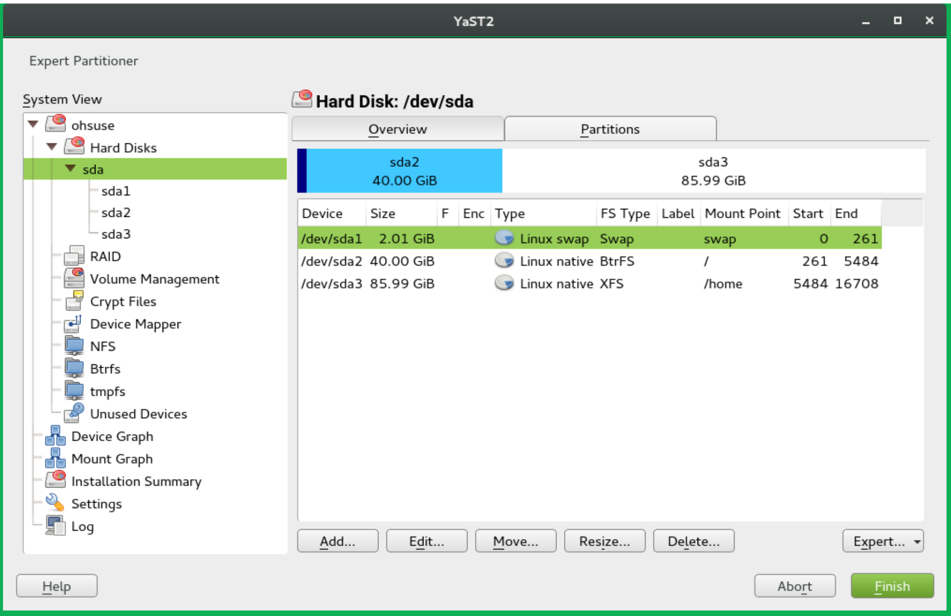
Με κλικ στο κουμπάκι Boot Loader της κατηγορίας System, έχουμε την ευκαιρία να αλλάξουμε τη συμπεριφορά του boot manager. Στο στιγμιότυπο αλλάζουμε το χρόνο εμφάνισης του μενού επιλογής λειτουργικού προς εκκίνηση, από τα 8 στα 5 δευτερόλεπτα. (Σοβαρά τώρα: Ποιος τρελός θα άφηνε το χρόνο εμφάνισης του μενού σε μη-πολλαπλάσιο του 5;)



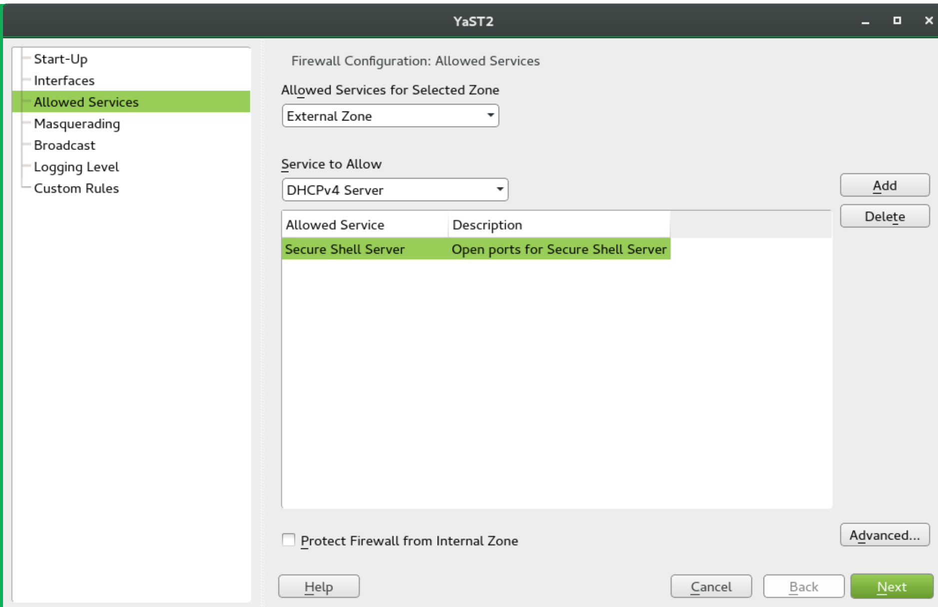
Δίνοντας System → Language μπορούμε να προσθέσουμε στο λειτουργικό και υποστήριξη για την Ελληνική γλώσσα.



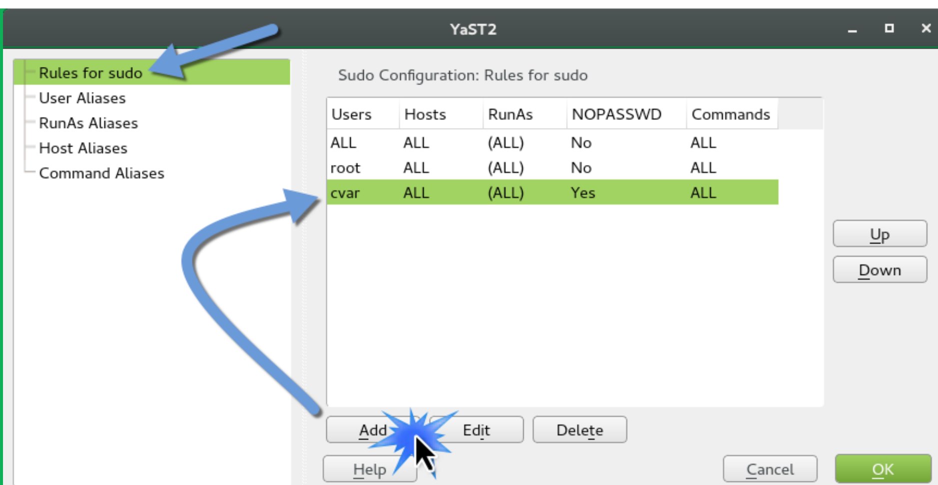
Η προσθήκη της Ελληνικής συνεπάγεται την εγκατάσταση μιας σειράς συνοδευτικών πακέτων (γραμματοσειρές, μεταφράσεις για διάφορες εφαρμογές κ.ο.κ.). Παρεμπιπτόντως, αφού το YaST εγκαταστήσει τα απαραίτητα πακέτα πηγαίνετε στον πίνακα ελέγχου του GNOME κι από την κατηγορία Personal επιλέξτε το Region & Language. Στο πλαίσιο Input Sources προσθέστε και το Ελληνικό πληκτρολόγιο.



Στο YaST, δίνοντας System   Partitioner καλούμε το module διαχείρισης δίσκων και διαμερισμάτων. Είναι ιδιαίτερα βολικό, ειδικά για τις φορές που προσθέτουμε νέο δίσκο στο σύστημα. (Σημείωση: Το screenshot είναι από VMware VM, όχι από το PC μας.)



Έλεγχος του firewall του openSUSE (Security & Users   Firewall), για όσους δεν τρελαίνονται να παίζουν με το iptables από τη γραμμή εντολών. Παρατηρήστε ότι, με βάση την επιλογή που κάναμε κατά το στάδιο της εγκατάστασης, η πρόσβαση στην υπηρεσία του SSH τώρα επιτρέπεται.



*Κάθε φορά που σε μια κονσόλα πληκτρολογούμε "sudo κάτι", ώστε να εκτελέσουμε το "κάτι" με δικαιώματα διαχειριστή συστήματος, ερωτόμαστε φυσικά για το password μας. Η ορθότητα της συγκεκριμένης πολιτικής δεν αμφισβητείται, αν όμως είμαστε *ο μόνος* χρήστης του συστήματος είναι κάπως βαρετό να πληκτρολογούμε κάθε λίγο και λιγάκι το password. Ευτυχώς, με την κατάλληλη παρέμβαση στο αρχείο /etc/sudoers είναι εφικτό για τον χρήστη μας (cvar) να καταφεύγει στο sudo *χωρίς* να πληκτρολογεί password. Η εν λόγω επέμβαση στο /etc/sudoers επιτυγχάνεται κι από το module του YaST ονόματι Sudo (είναι στην κατηγορία Security and Users). Αναλυτικότερα, πηγαίνουμε στην ενότητα Rules for sudo, πατάμε στο κουμπάκι Add και στο νέο παράθυρο που εμφανίζεται κάνουμε τις απαραίτητες επιλογές ώστε στο πλαίσιο "Sudo configuration: Rules for sudo" να έχουμε μια νέα γραμμή που μοιάζει με την πράσινη που υποδεικνύεται. (Προφανώς, στη θέση του "cvar" θα είναι το username του δικού σας χρήστη.)*

Skill: Intermediate
Tags: NAT, aliases, gateways, traceroute, packet capture, pfSense, OpenVPN

Η ζωή με τον OpenVPN-enabled router μας

Στο τεύχος 048 δείξαμε πώς στήνουμε έναν OpenVPN Access Server στο cloud και στη συνέχεια πώς ρυθμίζουμε έναν τοπικό pfSense-based router, ώστε να λειτουργεί ως πελάτης του. Το αποτέλεσμα είναι ότι όλα τα μηχανήματα και οι συσκευές πίσω από τον router βγαίνουν στο Internet μέσω ενός ασφαλούς κρυπτογραφημένου τούνελ. Θα περίμενε Κανείς ότι δεν θα είχαμε κάτι άλλο να συζητήσουμε επί του θέματος. Θα περίμενε λάθος, ο Κανείς αυτός.

του Χρήστου Βαρελά

Έτσι είναι τα πράγματα με το deltaHacker, φίλες και φίλοι. Συχνά ξεκινάμε με ένα ενδιαφέρον, κατά την κρίση μας, θέμα, μετά από ένα ή περισσότερα άρθρα φτάνουμε σε ένα ικανοποιητικό σημείο όπου όλα λειτουργούν σωστά κι όλοι είναι ευχαριστημένοι, ξαφνικά όμως συνειδητοποιούμε ότι υπάρχει κι ένα ολόκληρο υπό-σύμπαν για το οποίο δεν έχουμε γράψει ούτε μια λέξη ακόμα – ενώ θα έπρεπε. Αυτή τη φορά, αφού φροντίσαμε ώστε όλοι οι πελάτες του pfSense να βγαίνουν στο Internet *αυτόματα* μέσω του απομακρυσμένου OpenVPN Access Server, σκεφτήκαμε ότι είναι αδύνατον να κλείσουμε το θέμα αν πρώτα δεν δείξουμε πώς:

- βελτιστοποιούμε τη συμπεριφορά του Access Server,
- φέρνουμε στα μέτρα μας τη συμπεριφορά του pfSense router,
- βεβαιωνόμαστε ότι όλα δουλεύουν όπως ακριβώς θέλουμε.

Χωρίς άλλη καθυστέρηση ξεκινάμε με το NAT, ένα χρεωστούμενο από το άρθρο στο http://deltahacker.gr/actsubs-ovpn-for-lan.

Τι είναι αυτό το NAT και γιατί μας απασχόλησε;

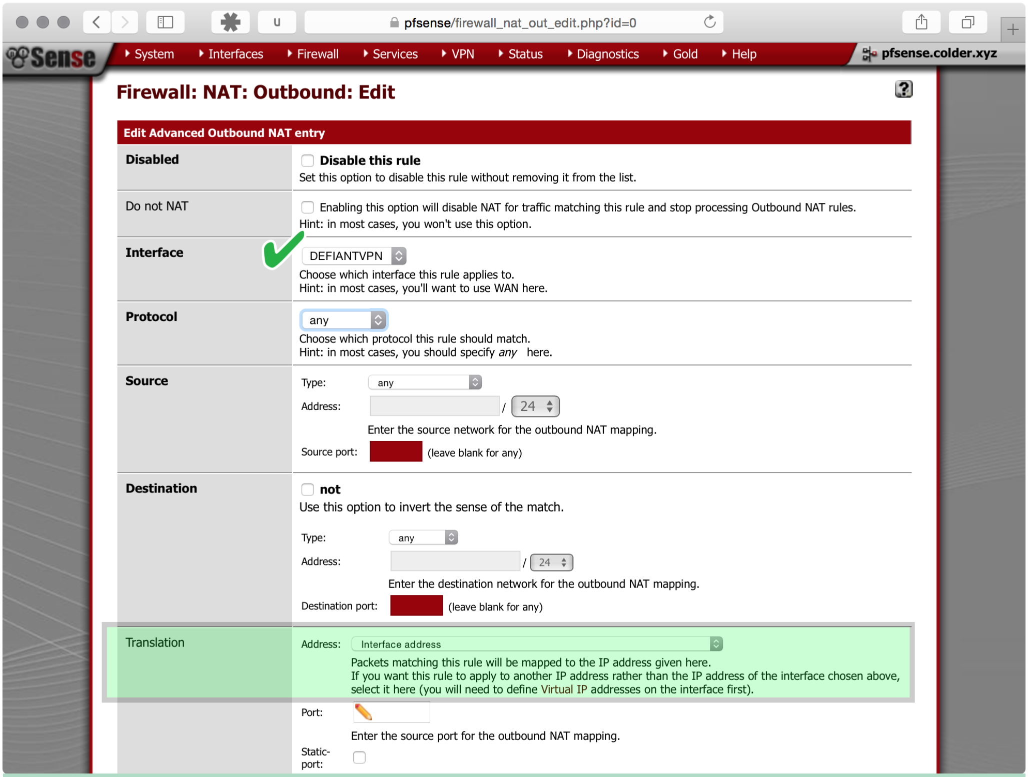
Μετά την πρώτη εγκαθίδρυση σύνδεσης μεταξύ pfSense router και OpenVPN Access Server, θα θυμόσαστε ίσως ότι όλες οι συσκευές πίσω από τον router έδειχναν ανίκανες να βγουν στο Internet. Η κατάσταση ομαλοποιήθηκε μόνον αφού προσθέσαμε στο firewall έναν κανόνα Outbound NAT για το DefiantVPN (έτσι έχουμε ονομάσει το network interface για τις συνδέσεις προς τον Access Server).

Γενικά, με τον όρο Network Address Translation ή απλά NAT αναφερόμαστε σε μεθόδους αντιστοίχισης μεταξύ δύο διαφορετικών IP spaces. Οι αντιστοιχίσεις πραγματοποιούνται αλλάζοντας κατάλληλα τα headers στα πακέτα IP, καθώς αυτά διέρχονται από συσκευές δρομολόγησης. Το NAT αρχικά χρησίμευε για τη διευκόλυνση της αναδρομολόγησης των πακέτων στα δίκτυα IP. Εδώ και πολλά χρόνια όμως αποτελεί ένα πολύτιμο εργαλείο για τη διαχείριση των δημόσιων διευθύνσεων IPv4, εν όψει μάλιστα της εξάντλησής τους.

Υπάρχουν πολλά είδη NAT και για να εξηγήσουμε πώς ακριβώς δουλεύουν οι σχετικές μέθοδοι αντιστοίχισης θα χρειαζόμασταν *τουλάχιστον* ένα εκτενές άρθρο. Στο πλαίσιο του παρόντος αρκεί να πούμε ότι, από τη σκοπιά του Μέσου Παπαδόπουλου (TM), το NAT μάς επιτρέπει να βγάζουμε στο Internet όσες από τις συσκευές μας θέλουμε, με *μία μόνο* δημόσια διεύθυνση IP: αυτή που έχει πάρει ο router μας από τον ISP.

Αναλυτικότερα, οι συσκευές μας συνδέονται –ενσύρματα ή ασύρματα– στον router και, χάρη στον DHCP server του, παίρνουν ωραιότατες αλλά non-routable διευθύνσεις IP, π.χ., της μορφής 192.168.0.0/24 ή της μορφής 10.0.0.0/24 (βλ. και http://deltahacker.gr/hownetsworkpart2b). Οι διευθύνσεις αυτές είναι μια χαρά για ένα τοπικό δίκτυο αλλά *όχι* για το Internet. Ευτυχώς, κάθε φορά που μία συσκευή χρειάζεται να συνδεθεί σε web site ή γενικά σε υπηρεσία του Διαδικτύου, ο router αλλάζει τη non-routable διεύθυνση πηγής (source IP) στα headers των σχετικών πακέτων και βάζει στη θέση της εκείνη που έχει πάρει από τον ISP και είναι routable για το Διαδίκτυο (ακριβέστερα: για το δίκτυο "μπροστά" από τον router). Έτσι, τα πακέτα είναι σε θέση να ταξιδεύουν Εκεί Έξω (TM) και μετά βασάνων και κόπων να φτάνουν στους προορισμούς τους. Όταν τώρα αποστέλλεται μια απάντηση από κάποιον ιντερνετικό server, εν είδει πακέτου IP, εκείνος που τη λαμβάνει είναι πάντα ο ακούραστος router μας. Χάρη σε σχετικό πίνακα που τηρεί, ο router ξέρει ότι ο πραγματικός αποδέκτης του πακέτου δεν είναι ο ίδιος αλλά η συσκευή που ξεκίνησε την επικοινωνία με τον server. Αλλάζει, λοιπόν, το δημόσιο IP στο πεδίο "destination IP" στο header του πακέτου, στη θέση του βάζει την "εσωτερική" διεύθυνση IP της συσκευής που είναι υπεύθυνη για όλη αυτή την αναστάτωση, κι αμέσως στέλνει το πακέτο προς τα εκεί που πρέπει.

Τώρα, κατά την αρχική ρύθμιση του pfSense οι κανόνες NAT για τα πακέτα που εξέρχονται από το WAN interface προστίθενται αυτόματα στο firewall ruleset. Δεν συμβαίνει όμως το ίδιο και για το network interface που δημιουργείται αμέσως μετά τη ρύθμιση του OpenVPN client. Το εν λόγω interface εμείς το ονομάσαμε DefiantVPN και για τον ορισμό κανόνων NAT που επιδρούν στα πακέτα που διέρχονται απ' αυτό δώσαμε Firewall → NAT → Outbound → Manual Outbound NAT rule generation (AON - Advanced Outbound NAT). Ο νέος κανόνας NAT που προσθέσαμε αφορά σε όλα τα πακέτα που εξέρχονται από το DefiantVPN, άσχετα από ποιο μηχάνημα ξεκινούν, ανεξαρτήτως του πρωτοκόλλου στο οποίο αφορούν (TCP, UDP, ICMP κ.ά.), κι ανεξαρτήτως του προορισμού τους. Στο screenshot που ακολουθεί προσέξτε την παράμετρο Address (περιοχή Translation), για την οποία επιλέξαμε την τιμή Interface address: Πρόκειται για τη διεύθυνση IP που αποδίδεται στο DefiantVPN από τον απομακρυσμένο OpenVPN Access Server (και για το δικό μας setup είναι η 172.27.232.2). Αυτή τη διεύθυνση βάζει στο πεδίο "source IP" των εξερχόμενων πακέτων, ο κανόνας NAT που ορίσαμε μόλις.



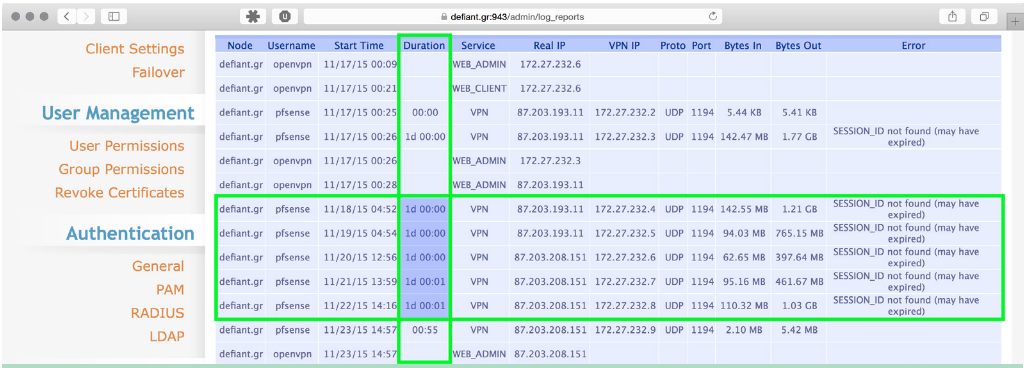
Ο νέος κανόνας NAT που προσθέσαμε χειροκίνητα στο firewall ruleset του pfSense. Παρουσία του διασφαλίζεται ότι στο πεδίο "source IP", στο header των πακέτων που εξέρχονται από το DefiantVPN, υπάρχει η διεύθυνση IP που ο Access Server έχει αποδώσει στο προαναφερθέν network interface. Παρόμοιοι κανόνες NAT που αφορούν στο WAN interface είχαν προστεθεί αυτόματα, κατά την αρχική ρύθμιση του pfSense.

Η σύνδεση με τον Access Server διακόπτεται :/

Μετά τη ρύθμιση του pfSense router ώστε να λειτουργεί ως client για τον OpenVPN Access Server, πιθανώς θα παρατηρήσατε ότι η σύνδεση προς το απομακρυσμένο μηχάνημα έχει μια τάση να διακόπτεται. Αν κάνετε όπως εμείς κι αφήνετε τον OpenVPN client να λειτουργεί αδιάκοπα, είναι *βέβαιο* ότι θα το έχετε παρατηρήσει. Δεν πρόκειται για φαινόμενο που συμβαίνει τυχαία, π.χ., εξαιτίας κάποιου bug. Κάθε άλλο: Αυτή ακριβώς είναι η προκαθορισμένη συμπεριφορά του Access Server, για τα profiles χρηστών με το auto-login απενεργοποιημένο. (Οι χρήστες με τέτοια προφίλ, εκτός από το να κατέχουν το κατάλληλο ιδιωτικό κλειδί και πιστοποιητικό, κατά τη σύνδεσή τους πρέπει να παρέχουν username και password.)

Εξ ορισμού, λοιπόν, ο Access Server διακόπτει τις συνδέσεις των προφίλ χωρίς auto-login κάθε 86.400 δευτερόλεπτα, δηλαδή κάθε 24 ώρες. Ευτυχώς, μπορούμε να αλλάξουμε τη σχετική παράμετρο και να της αποδώσουμε μια πολύ μεγάλη τιμή, ώστε στην πράξη οι αποσυνδέσεις να μην έχουν καμία ευκαιρία να συμβαίνουν. Θέτοντας το χρόνο για την αποσύνδεση, π.χ., στα 31.104.000 δευτερόλεπτα (360 μέρες), είναι

βέβαιο ότι πριν ο Access Server προλάβει να διακόψει συνδέσεις θα έχουμε κάνει εμείς κάποιο reboot, π.χ., λόγω κάποιου major upgrade στο pfSense ή λόγω αναβάθμισης του πυρήνα στο λειτουργικό που τρέχει το VPS του Access Server.



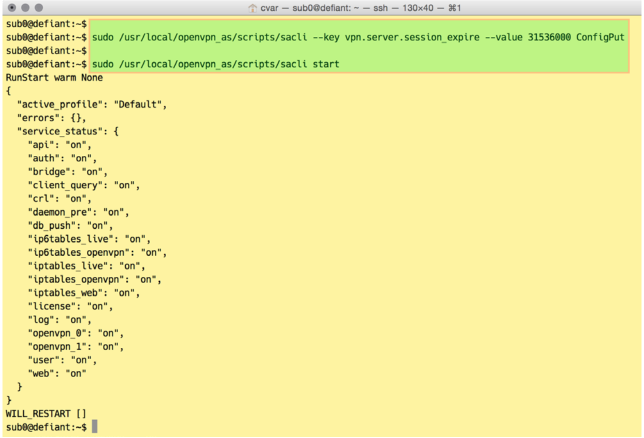
Node	Username	Start Time	Duration	Service	Real IP	VPN IP	Proto	Port	Bytes In	Bytes Out	Error
defiant.gr	openvpn	11/17/15 00:09		WEB_ADMIN	172.27.232.6						
defiant.gr	openvpn	11/17/15 00:21		WEB_CLIENT	172.27.232.6						
defiant.gr	pfsense	11/17/15 00:25	00:00	VPN	87.203.193.11	172.27.232.2	UDP	1194	5.44 KB	5.41 KB	
defiant.gr	pfsense	11/17/15 00:26	1d 00:00	VPN	87.203.193.11	172.27.232.3	UDP	1194	142.47 MB	1.77 GB	SESSION_ID not found (may have expired)
defiant.gr	openvpn	11/17/15 00:26		WEB_ADMIN	172.27.232.3						
defiant.gr	openvpn	11/17/15 00:28		WEB_ADMIN	87.203.193.11						
defiant.gr	pfsense	11/18/15 04:52	1d 00:00	VPN	87.203.193.11	172.27.232.4	UDP	1194	142.55 MB	1.21 GB	SESSION_ID not found (may have expired)
defiant.gr	pfsense	11/19/15 04:54	1d 00:00	VPN	87.203.193.11	172.27.232.5	UDP	1194	94.03 MB	765.15 MB	SESSION_ID not found (may have expired)
defiant.gr	pfsense	11/20/15 12:56	1d 00:00	VPN	87.203.208.151	172.27.232.6	UDP	1194	62.65 MB	397.64 MB	SESSION_ID not found (may have expired)
defiant.gr	pfsense	11/21/15 13:59	1d 00:01	VPN	87.203.208.151	172.27.232.7	UDP	1194	95.16 MB	461.67 MB	SESSION_ID not found (may have expired)
defiant.gr	pfsense	11/22/15 14:16	1d 00:01	VPN	87.203.208.151	172.27.232.8	UDP	1194	110.32 MB	1.03 GB	SESSION_ID not found (may have expired)
defiant.gr	pfsense	11/23/15 14:57	00:55	VPN	87.203.208.151	172.27.232.9	UDP	1194	2.10 MB	5.42 MB	
defiant.gr	openvpn	11/23/15 14:57		WEB_ADMIN	87.203.208.151						

Παρατηρώντας το log file του OpenVPN Access Server μέσα από web panel διαχείρισης, εύκολα διαπιστώνουμε ότι ο server αποσυνδέει τον έναν και μοναδικό του client κάθε 24 ώρες. Ο εν λόγω client είναι ο pfSense router μας κι αυτή η κατάσταση με τις αποσυνδέσεις πρέπει να σταματήσει, αφού δημιουργούνται προβλήματα στις συσκευές πίσω από τον router.

Προκειμένου ν' αλλάξουμε το χρόνο για την αποσύνδεση, συνδεόμαστε στο VPS του OpenVPN Access Server μέσω SSH και πληκτρολογούμε:

```
sub0@defiant:~$ sudo /usr/local/openvpn_as/scripts/sacli --key vpn.server.
session_expire --value 31536000 ConfigPut
sub0@defiant:~$ sudo /usr/local/openvpn_as/scripts/sacli start
```

Η παράμετρος που επηρεάσαμε είναι η vpn.server.session_expire. Παρεμπιπτόντως, όλες οι παράμετροι που καθορίζουν τη συμπεριφορά του OpenVPN Access Server τηρούνται στην SQLite database ονόματι config.db, κάτω από το /usr/local/openvpn_as/etc/db.




```
sub0@defiant:~$
sub0@defiant:~$ sudo /usr/local/openvpn_as/scripts/sacli --key vpn.server.session_expire --value 31536000 ConfigPut
sub0@defiant:~$
sub0@defiant:~$ sudo /usr/local/openvpn_as/scripts/sacli start
RunStart warm None
{
  "active_profile": "Default",
  "errors": {},
  "service_status": {
    "api": "on",
    "auth": "on",
    "bridge": "on",
    "client_query": "on",
    "crl": "on",
    "daemon_pre": "on",
    "db_push": "on",
    "ip6tables_live": "on",
    "ip6tables_openvpn": "on",
    "iptables_live": "on",
    "iptables_openvpn": "on",
    "iptables_web": "on",
    "license": "on",
    "log": "on",
    "openvpn_0": "on",
    "openvpn_1": "on",
    "user": "on",
    "web": "on"
  }
}
WILL_RESTART []
sub0@defiant:~$
```

*Έχοντας συνδεθεί μέσω SSH στο VPS που τρέχει ο OpenVPN Access Server, αλλάζουμε την τιμή αποσύνδεσης για τους χρήστες του Access Server με προφίλ *χωρίς* auto-login. Στο εξής, οι αυτόματες αποσυνδέσεις θα γίνονται κάθε ένα χρόνο. Στο μεταξύ, είναι σχεδόν σίγουρο πως ούτως ή άλλως θα έχουμε επανεκκινήσει το pfSense ή το λειτουργικό του VPS, π.χ., λόγω αναβάθμισης του πυρήνα.*

Επιλεκτική δρομολόγηση μέσω VPN

Η δρομολόγηση της δικτυακής κίνησης μέσω του απομακρυσμένου Access Server συχνά έχει αρνητική επίπτωση στην ταχύτητα. Η επίπτωση αυτή άλλοτε είναι πρακτικά αμελητέα, άλλες φορές όμως δεν περνά απαρατήρητη. Όλα εξαρτώνται από το είδος της διαδικτυακής υπηρεσίας που προσπελαύνουμε. Παράδειγμα: Για τυπικό web browsing, το πιθανότερο είναι να μην αντιλαμβανόμαστε την όποια μείωση στην ταχύτητα. Αν βέβαια ο web server που επισκεπτόμαστε είναι γεωγραφικά κοντά μας ή/και δεν διαθέτει το καλύτερο bandwidth, το να τον προσεγγίζουμε, π.χ., μέσω data center στη Νέα Υόρκη, σίγουρα απέχει από το βέλτιστο – πάντα όσον αφορά στην ταχύτητα. (Ο OpenVPN Access Server που διαχειριζόμαστε κατοικεί σε data center στη Νέα Υόρκη.) Άλλο παράδειγμα: Στο τοπικό μας δίκτυο ίσως έχουμε ένα μηχάνημα το οποίο χρησιμοποιούμε κυρίως για online gaming, οπότε ειδικά αυτό καλό είναι να μη βαίνει έξω μέσω VPN. Μπορεί βέβαια να ισχύει και το αντίστροφο: μέσω Access Server να θέλουμε να βγαίνουν στο Internet συγκεκριμένα μόνο μηχανήματα. Η καλύτερη λύση για σενάρια σαν τα προαναφερθέντα, είναι να προσθέσουμε στο ruleset του firewall κανόνες που θα φροντίζουν για ένα ή περισσότερα από τα ακόλουθα:

- όταν επισκεπτόμαστε συγκεκριμένα sites να μην τα προσεγγίζουμε μέσω του ISP
- όταν επισκεπτόμαστε συγκεκριμένα sites να τα προσεγγίζουμε μέσω του Access Server
- μόνο συγκεκριμένες συσκευές του τοπικού δικτύου να βγαίνουν έξω μέσω του ISP
- μόνο συγκεκριμένες συσκευές του τοπικού δικτύου να βγαίνουν έξω μέσω του Access Server

Τα προηγούμενα τα πετυχαίνουμε προσθέτοντας τους κατάλληλους κανόνες στο firewall του pfSense, για το network interface που βλέπουν οι πελάτες και βεβαίως με τη σωστή σειρά. Είναι πολύ πιθανό να έχουμε πολλές υπηρεσίες, συσκευές ή sites για τα οποία επιθυμούμε εξαιρέσεις μέσω κανόνων. Ο βέλτιστος τρόπος προκειμένου να τους ορίσουμε και να τους διαχειριζόμαστε είναι με τη βοήθεια των λεγόμενων aliases.

Τα aliases του pfSense

Τα aliases μπορούμε να τα φανταζόμαστε ως λίστες με ένα ή περισσότερα ομοειδή στοιχεία. Αναφερόμενοι σε στοιχεία εννοούμε ports, hosts ή ολόκληρα δίκτυα. Ένα alias, για παράδειγμα, μπορεί να ισούται με τη λίστα {22, 80, 443, 1194}, όπου τα στοιχεία της είναι TCP ports που είναι προσβάσιμα από το Intetnet. Άλλο alias ίσως ταυτίζεται με τη λίστα {192.168.10.5, 192.168.10.95}, όπου τα μηχανήματα με διευθύνσεις 192.168.10.5 και 192.168.10.95 βγαίνουν στον έξω κόσμο πάντα μέσω VPN. Κάποιο άλλο alias μπορεί να ταυτίζεται με τη λίστα {192.168.100.0/24, 192.168.150.0/24}, ώστε να περιγράφει τα δίκτυα για τα οποία η πρόσβαση στο Internet επιτρέπεται μόνο κατά συγκεκριμένα χρονικά διαστήματα μέσα στο εικοσιτετράωρο. Τα aliases με hosts, αντί για IPs επιτρέπεται να έχουν και FQDNs. Έτσι, είναι δυνατόν να διαθέτουμε, π.χ., ένα alias που ισούται με τη λίστα {deltahacker.gr, parabing.com, colder.xyz}, ώστε σε καθένα από αυτά τα sites να φτάνουμε πάντα μέσω του ISP μας κι όχι μέσω απομακρυσμένου VPN server. Στην περίπτωση που σε ένα FQDN αντιστοιχούν περισσότερα από ένα IPs, στη λίστα λαμβάνονται υπόψη όλα.

cvar — bash — 85×35 — ⌘1

```
mbpr15:~ cvar$
mbpr15:~ cvar$ dig softpedia.com

; <<>> DiG 9.8.3-P1 <<>> softpedia.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 40849
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 3, ADDITIONAL: 3

;; QUESTION SECTION:
;softpedia.com.                 IN      A

;; ANSWER SECTION:
softpedia.com.          3600    IN      A       64.225.158.192
softpedia.com.          3600    IN      A       64.225.158.189
softpedia.com.          3600    IN      A       64.225.158.190
softpedia.com.          3600    IN      A       64.225.158.191

;; AUTHORITY SECTION:
softpedia.com.          2304    IN      NS      ns3.softpedia.com.
softpedia.com.          2304    IN      NS      ns2.softpedia.com.
softpedia.com.          2304    IN      NS      ns.softpedia.com.

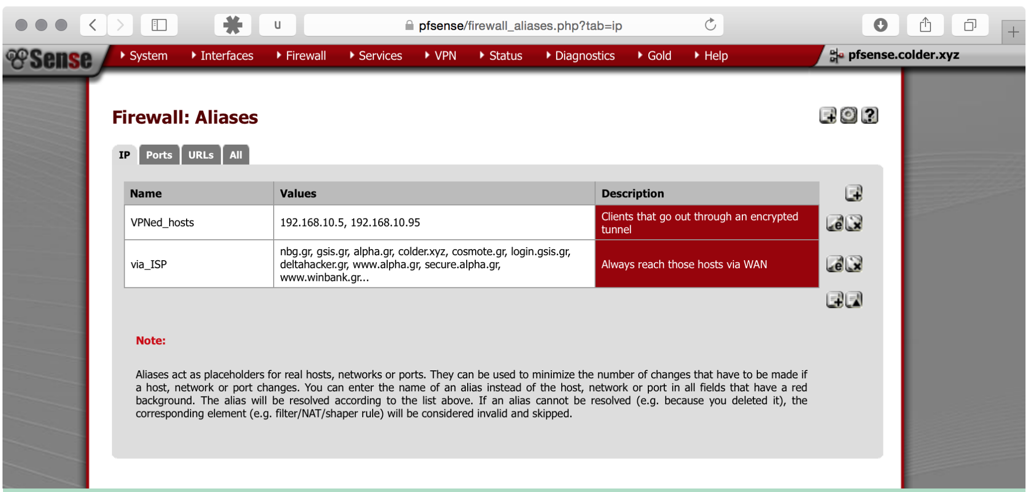
;; ADDITIONAL SECTION:
ns3.softpedia.com.      2304    IN      A       64.225.152.196
ns2.softpedia.com.      2304    IN      A       64.225.152.196
ns.softpedia.com.       2304    IN      A       128.140.224.120

;; Query time: 526 msec
;; SERVER: 192.168.10.254#53(192.168.10.254)
;; WHEN: Wed Dec  2 20:11:08 2015
;; MSG SIZE  rcvd: 196

mbpr15:~ cvar$
```

Σε περίπτωση που σ' ένα alias υπάρχει FQDN στο οποίο αντιστοιχούν περισσότερες από μία διευθύνσεις IP, όπως, π.χ., συμβαίνει με το softpedia.com, στο alias θα είναι σαν να περιλαμβάνονται όλες αυτές οι διευθύνσεις.

Το πόσο βολικά είναι τα aliases καταδεικνύεται όταν τα χρησιμοποιούμε σε κανόνες του firewall. Περισσότερα επ' αυτού θα δούμε σε πολύ λίγο. Προς το παρόν, ας υπογραμμίσουμε την ευκολία που παρέχουν: Χάρη σ' αυτά, κάθε φορά που ένα ή περισσότερα ports/hosts/δίκτυα πρέπει ν' αλλάξουν, οι συνεπακόλουθες αλλαγές στα rulesets του firewall ελαχιστοποιούνται. Το μόνο που απαιτείται από μέρους μας είναι να ορίζουμε aliases έχοντας ξεκαθαρισμένο το ρόλο τους. Βοηθά, βεβαίως, να τους δίνουμε και περιγραφικά ονόματα. Περιττό επίσης να σημειώσουμε ότι στα aliases μπορούμε να προσθέτουμε ή να αφαιρούμε μέλη όποτε θέλουμε, και η ισχύς των εμπλεκομένων κανόνων θα επεκτείνεται ή θα περιορίζεται αντιστοίχως. Όμως ας αφήσουμε τη γενική συζήτηση κι ας δούμε δύο παραδείγματα aliases, τα οποία έχουμε ορισμένα στον δικό μας pfSense router.



Για τον ορισμό ενός νέου alias ή την τροποποίηση κάποιου υπάρχοντος, από το web panel του pfSense δίνουμε Firewall Aliases. Στην καρτέλα IP διακρίνονται τα δύο aliases που έχουμε ορίσει στο pfSense box μας, προκειμένου να καθορίσουμε τις υπηρεσίες και τα sites στα οποία θέλουμε να φτάνουμε μέσω του ISP, καθώς και τις συσκευές που θέλουμε να βγαίνουν στο Internet πάντα μέσω του απομακρυσμένου OpenVPN Access Server. Διαβάστε στη συνέχεια τις λεπτομέρειες για την υλοποίηση αυτής της πολιτικής.

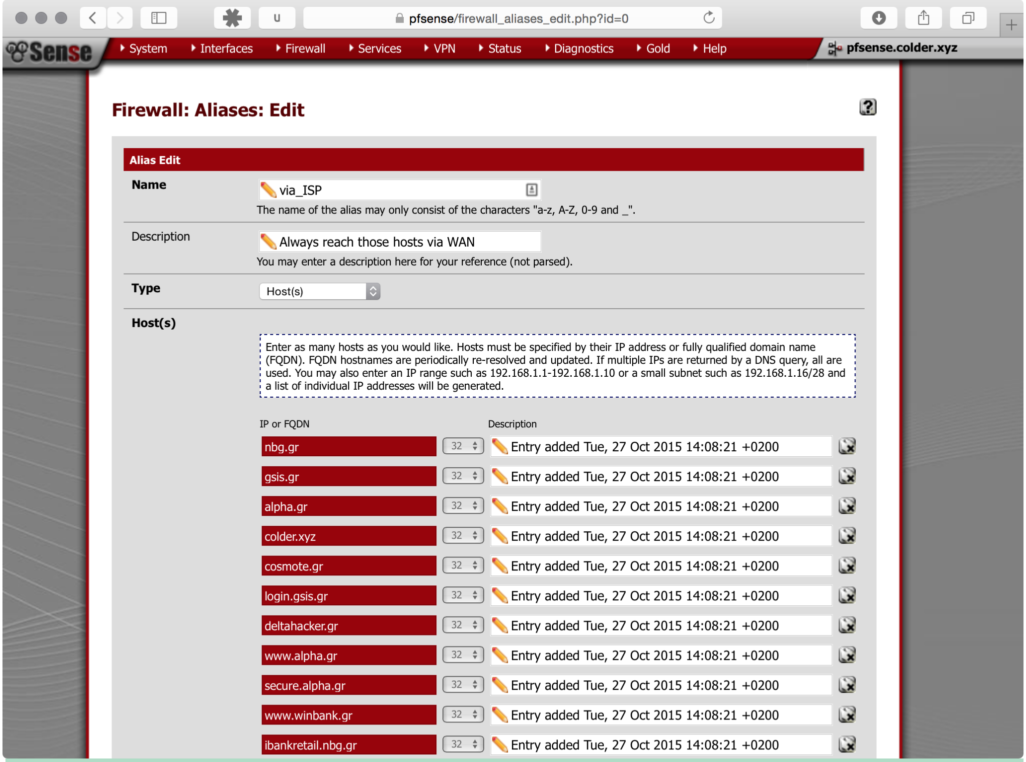
Εφαρμογή 1: Παράκαμψη VPN για συγκεκριμένα sites

Μεταξύ των υπηρεσιών και των sites που εμείς χρησιμοποιούμε κι επισκεπτόμαστε συχνά, υπάρχουν ορισμένα στα οποία αφενός δεν έχει πολύ νόημα να φτάνουμε μέσω VPN tunnel, αφετέρου η πρόσβαση γίνεται κάπως αργά μέσω του απομακρυσμένου server. Στα προαναφερθέντα sites συγκαταλέγονται τα συστήματα web banking ελληνικών τραπεζών, το TAXIS, εκείνα κάποιων τηλεπικοινωνιακών φορέων κ.ά. Δημιουργήσαμε έτσι ένα νέο alias ονόματι via_ISP, το οποίο περιλαμβάνει όλα αυτά τα sites κι όχι μόνο. Επιπλέον, έχει και κάποια, όπως, π.χ., το ruv.is, τα οποία φιλοξενούνται σε servers στο εξωτερικό και η πρόσβαση από Θεσσαλονίκη μέσω Νέας Υόρκης γίνεται αργά — ειδικά όταν μιλάμε για video streaming.

Μπροστά από το pfSense box βρίσκεται το ADSL modem/router που έχουμε πάρει από τον ISP. Το IP που έχει το LAN interface του modem/router είναι 192.168.1.1 και μερικές φορές χρειάζεται να συνδεόμαστε στο web panel της συσκευής, γι' αυτό και στο alias ονόματι via_ISP έχουμε συμπεριλάβει το 192.168.1.1. (Σ' αυτή τη διεύθυνση είναι αδύνατο να φτάνουμε μέσω του Access Server.) Στο via_ISP συμπεριλαμβάνεται και το defiant.gr, το οποίο είναι το FQDN του VPS όπου κατοικεί ο Access Server. Σ' αυτό το VPS θέλουμε, προφανώς, να φτάνουμε από οποιαδήποτε συσκευή, ασχέτως του αν βγαίνει στο Internet μέσω ISP ή μέσω Access Server.

Στη λίστα του via_ISP υπάρχει και το colder.xyz: Πρόκειται για ένα VPS σε data center στη Φρανκφούρτη που φιλοξενεί το ομώνυμο static site, καθώς κι έναν mail server που λειτουργούμε εκεί (βλ. και http://deltahacker.gr/?p=14096). Για το static site δεν μας πειράζει και τόσο, όμως δεν βλέπουμε το λόγο να διακινούμε την ηλεκτρονική μας αλληλογραφία μέσω Νέας Υόρκης.

Αφού ορίσαμε το alias ονόματι via_ISP, έμενε να προσθέσουμε έναν σχετικό κανόνα στο ruleset του pfSense firewall — βεβαίως για το κατάλληλο network interface. Περισσότερα επ' αυτού σε πολύ λίγο.

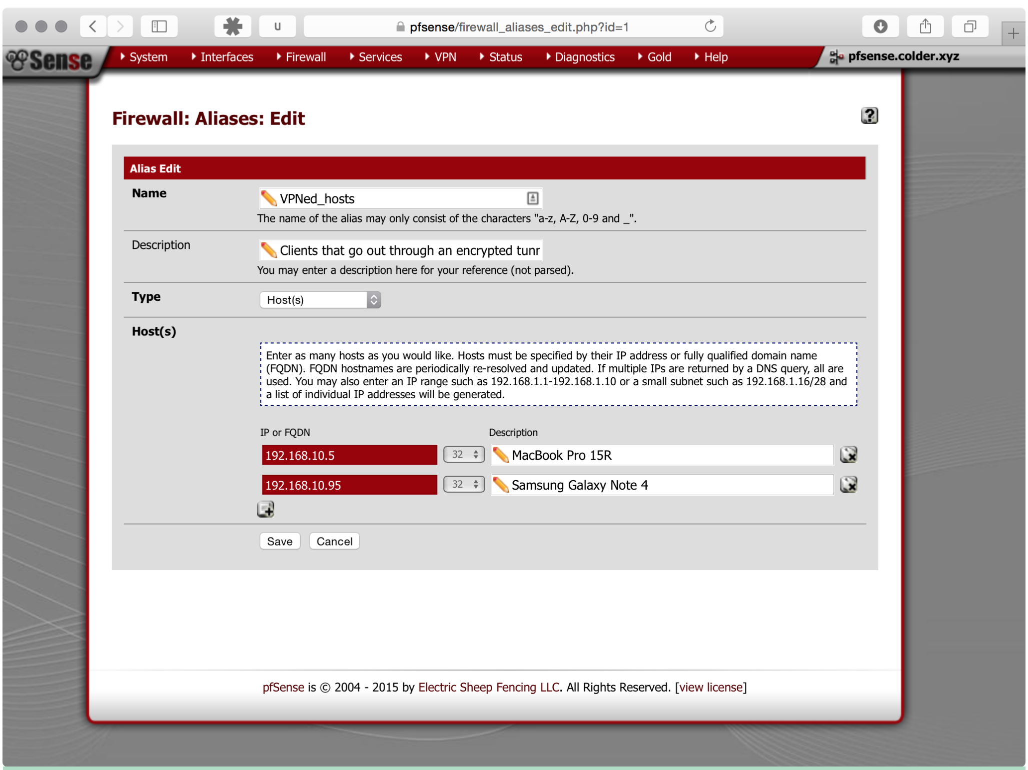


Μέρος των περιεχομένων του alias ονόματι via_ISP, το οποίο περιλαμβάνει υπηρεσίες και sites στα οποία θέλουμε να φτάνουμε πάντοτε μέσω του ISP μας κι όχι μέσω του απομακρυσμένου OpenVPN Access Server.

Εφαρμογή 2: Χρήση VPN για συγκεκριμένα hosts

Στο τοπικό μας δίκτυο πίσω από το pfSense, αυτή τη στιγμή υπάρχει ένας δικτυακός εκτυπωτής, ένα tablet, δύο smartphones, δύο laptops, ένα PC με το ProxMox VE, ένα VM με Ubuntu Server σε ρόλο Dropbox node, καθώς κι ένα VM με Ubuntu Desktop που έχει χρέη Bitcoin full node. Μιλάμε, μ' άλλα λόγια, για εννέα διαφορετικούς clients. Για λόγους που δεν χρειάζεται να παραθέσουμε τώρα, δύο μόνο από τις εννέα αυτές συσκευές έχει νόημα (και είναι επιθυμητό) να βγαίνουν διαρκώς στο Internet μέσω Access Server: το ένα από τα δύο laptops και το ένα από τα δύο smartphones. Ακριβώς γι' αυτό, λοιπόν, ορίσαμε ένα alias που ονομάσαμε VPNed_hosts και περιλαμβάνει τις δύο διευθύνσεις IP που οι δύο αυτές συσκευές παίρνουν από τον DHCP server του pfSense. (Εννοείται πως έχουμε ήδη μεριμνήσει, μέσα από το web panel του pfSense, ώστε οι υπό συζήτηση συσκευές να παίρνουν πάντοτε τις ίδιες διευθύνσεις IP.)

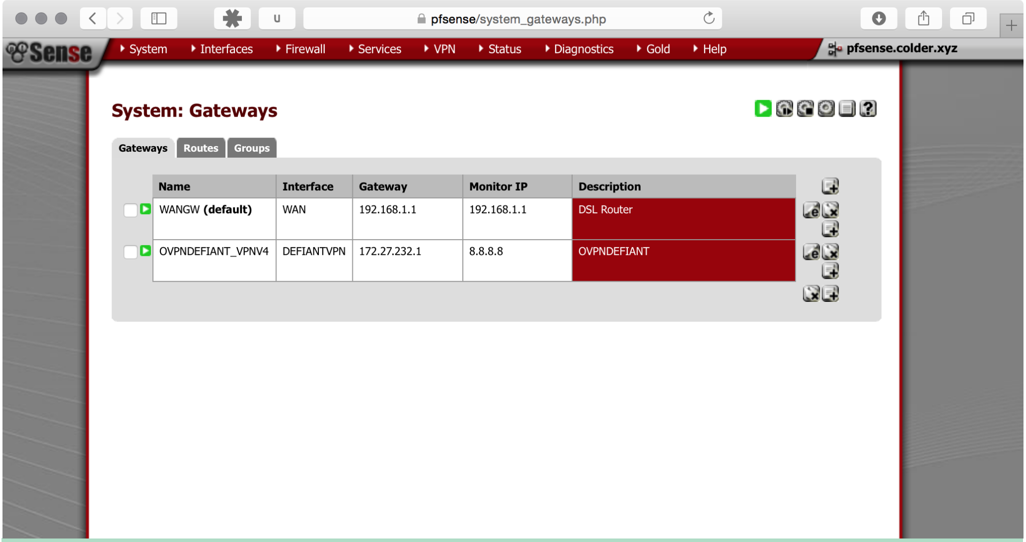
Είδαμε τα δύο aliases του pfSense box, εξηγήσαμε και το λόγο ύπαρξης καθενός. Στην επόμενη ενότητα παραθέτουμε και τους σχετικούς κανόνες στο firewall του pfSense, ώστε να υλοποιείται η επιθυμητή πολιτική διαχείρισης της δικτυακής κυκλοφορίας.



*Το alias ονόματι VPNed_hosts περιλαμβάνει τις διευθύνσεις IP των δύο συσκευών που επιθυμούμε να βγαίνουν στο Internet *πάντοτε* μέσω του απομακρυσμένου OpenVPN Access Server. Όλες οι άλλες συσκευές βγαίνουν απευθείας, δηλαδή παρακάμπτουν το κρυπτογραφημένο τούνελ από το pfSense box έως το VPS του Access Server.*

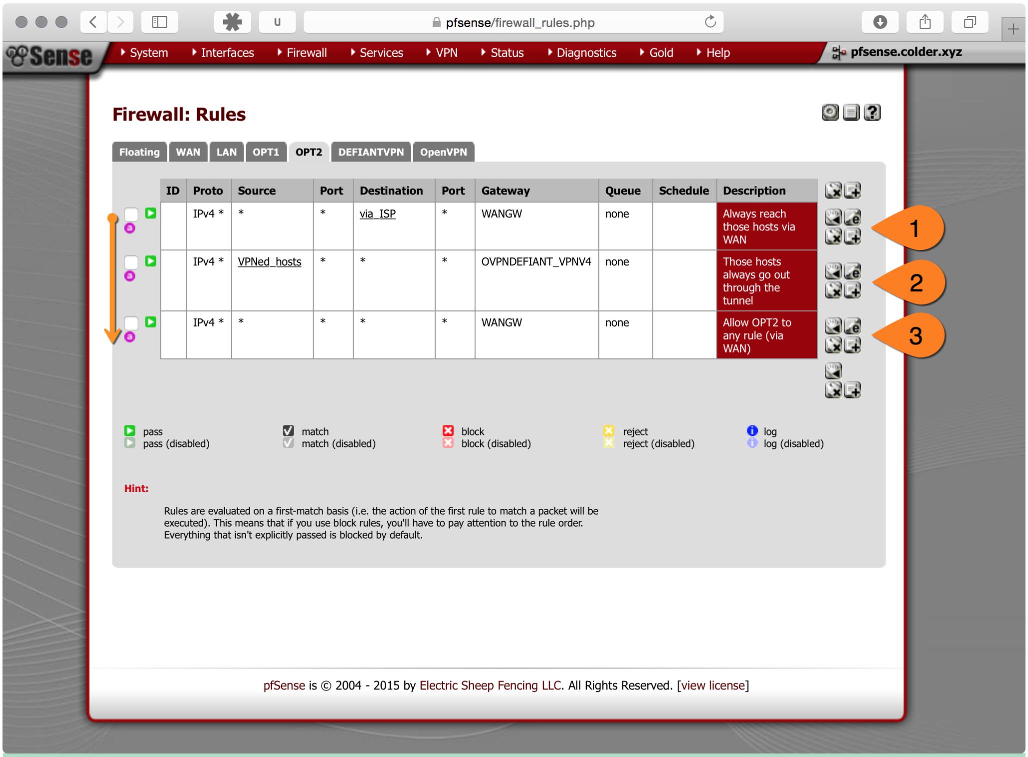
Κανόνες στο firewall

Από το web panel του pfSense επιλέγουμε System → Routing κι εστιάζουμε την προσοχή μας στην καρτέλα Gateways. Μετά την πρώτη εγκατάσταση και ρύθμιση του pfSense υπάρχει μία μόνο προκαθορισμένη πύλη, με όνομα WANGW: Πρόκειται για εκείνη που χρησιμοποιεί το WAN interface του pfSense ώστε οι συσκευές πίσω από τον router να βγαίνουν στο Internet. Αυτή η πύλη οδηγεί απευθείας στον ISP μας. Μετά όμως τη ρύθμιση του client για τον OpenVPN Access Server, στο pfSense διατίθεται και η πύλη με όνομα OVPNDEFIANT_VPNV4 – ή τουλάχιστον αυτό είναι το όνομά της για τη δική μας εγκατάσταση. Η εν λόγω πύλη χρησιμοποιείται από το DefiantVPN interface κι όσες συσκευές τη χρησιμοποιούν δεν βγαίνουν στο Internet απευθείας από τον ISP, αλλά αφού πρώτα περάσουν από το κρυπτογραφημένο τούνελ που ξεκινά από το pfSense και καταλήγει στον Access Server.



Τα δύο gateways του δικού μας pfSense box. Από το WANGW οι πελάτες βγαίνουν απευθείας στο Internet, μέσω του ISP μας. Από το OPENVPNDEFIANT_VPNV4 οι πελάτες βγαίνουν στο Internet από τον OpenVPN Access Server, ταξιδεύοντας μέσα από το κρυπτογραφημένο τούνελ που υφίσταται μεταξύ pfSense box κι απομακρυσμένου VPS.

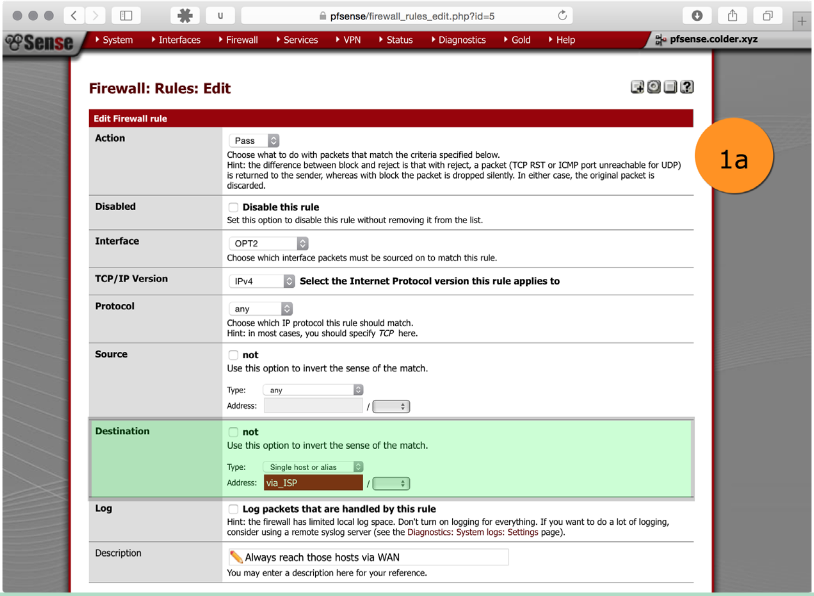
Τις δύο προαναφερθείσες πύλες, WANGW και OPENVPNDEFIANT_VPNV4, πρέπει να έχουμε υπόψη κατά τη σύνταξη των κανόνων δρομολόγησης της κίνησης. Τώρα, για την προσθήκη των κανόνων δίνουμε Firewall → Rules. Οι νέοι κανόνες θα αφορούν στο network interface που έχουν μπροστά τους οι πελάτες του router, αφού ενδιαφερόμαστε για τα πακέτα που εξέρχονται από το τοπικό δίκτυο. Κατά πάσα πιθανότητα μιλάμε για το LAN interface. Υπάρχουν όμως κι άλλες δυνατότητες. Για παράδειγμα, στο δικό μας setup ασχοληθήκαμε με το OPT2 interface, το οποίο αποτελεί bridge των LAN και OPT1. Σε κάθε περίπτωση, στη σελίδα "Firewall: Rules" κάντε κλικ στην καρτέλα του κατάλληλου για την εγκατάστασή σας network interface. Δείτε στα screenshots που ακολουθούν τους κανόνες που ισχύουν για το δικό μας interface (το OPT2), διαβάστε βεβαίως και τις αντίστοιχες περιγραφές.



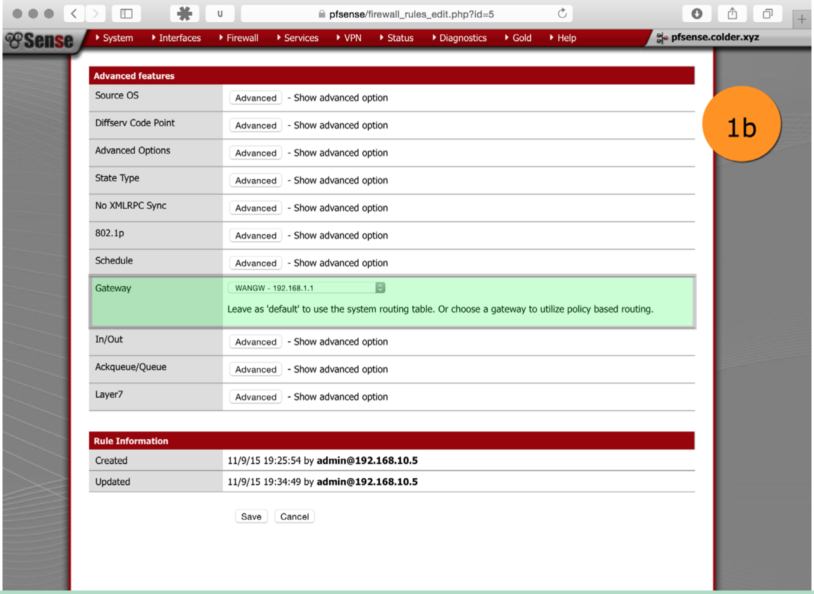
Ιδού οι τρεις κανόνες του firewall για το OPT2, το network interface που βλέπουν οι πελάτες του pfSense. Η σειρά των κανόνων έχει σημασία, αφού εφαρμόζονται από πάνω προς τα κάτω, ο πρώτος κανόνας που "ταιριάζει" σε εισερχόμενο πακέτο ενεργοποιείται, ενώ όλοι οι άλλοι από "κάτω", αν υπάρχουν, αγνοούνται. Έτσι, οι τρεις εικονιζόμενοι κανόνες έχουν τα ακόλουθα αποτελέσματα:

- *αν ένα πακέτο, απ' όποιον client κι αν προέρχεται, προορίζεται για κάποιον από τους hosts που παρατίθενται στο alias ονόματι via_ISP, τότε στείλε το έξω μέσω του WANGW gateway (δηλαδή όχι μέσω του κρυπτογραφημένου τούνελ) – κι αγνόησε τους κανόνες από κάτω*
- *αν ένα πακέτο προέρχεται από κάποιον εκ των clients που παρατίθενται στο alias ονόματι VPNed_hosts, τότε στείλε το έξω μέσω του OVPNDEFIANT_VPNV4 gateway (δηλαδή μέσω του κρυπτογραφημένου τούνελ) – κι αγνόησε τους κανόνες από κάτω*
- *αν ένα πακέτο προέρχεται από έναν οποιονδήποτε άλλον client, τότε στείλε το έξω μέσω του WANGW gateway (δηλαδή όχι μέσω του κρυπτογραφημένου τούνελ)*

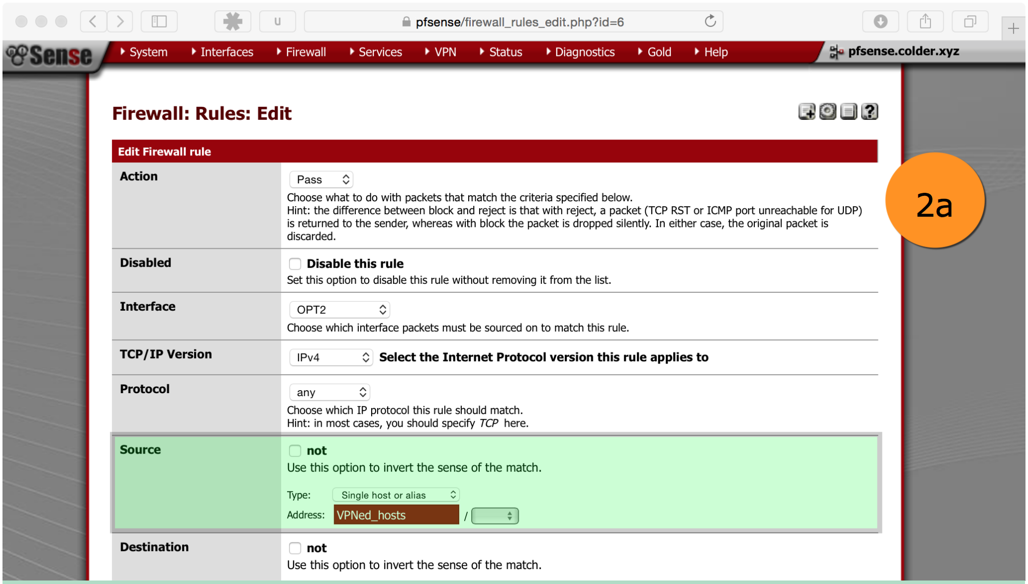
Θα μπορούσε κάποιος να ισχυριστεί ότι 1ος κανόνας είναι περιττός και ότι ο 2ος κι ο 3ος θα ήταν αρκετοί. Στην πραγματικότητα όμως η παρουσία του 1ου κανόνα είναι απαραίτητη, ώστε αν κάποιο πακέτο προορίζεται για κάποιον host από το via_ISP να βγαίνει έξω μέσω WANGW ακόμη κι όταν προέρχεται από client της λίστας VPNed_hosts.



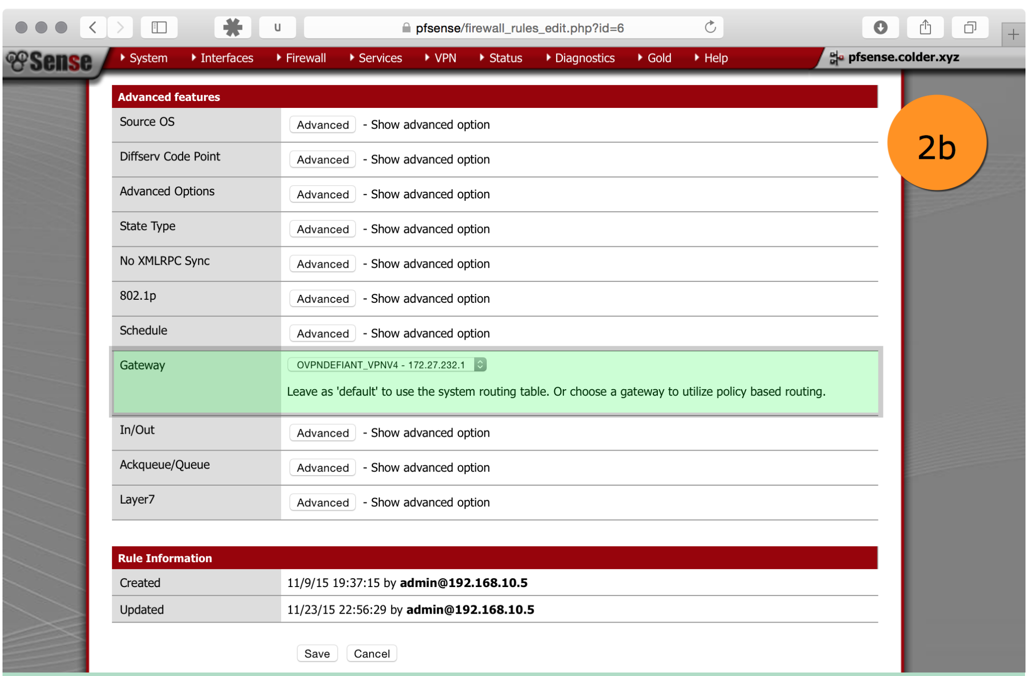
Ζουμ στις παραμέτρους του 1ου κανόνα. Προσέξτε την ενότητα Destination, όπου θέσαμε Type = Single host or alias και στη θυρίδα Address πληκτρολογήσαμε το όνομα του alias με τα hosts στα οποία θέλουμε να φτάνουμε μέσω WANGW (via_ISP).



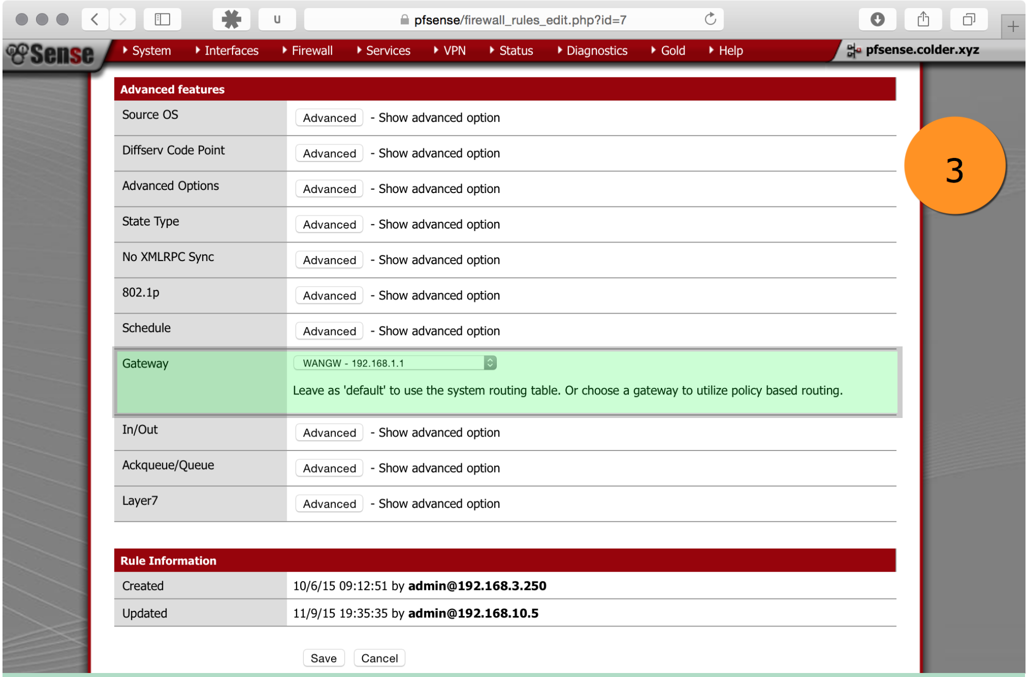
Λίγο πιο κάτω, στην περιοχή με τα Advanced features του κανόνα, δεν λησμονήσαμε να θέσουμε Gateway = WANGW.



Ζουμ στις παραμέτρους του 2ου κανόνα. Αυτή τη φορά εστιάσαμε την προσοχή μας στην ενότητα Source. Θέσαμε και πάλι Type = Single host or alias αλλά στη θυρίδα Address πληκτρολογήσαμε VPNed_hosts, το οποίο είναι το όνομα που έχουμε δώσει στο alias με τα IPs των clients που επιθυμούμε να βγαίνουν στο Internet μέσω του Access Server.



Στην περιοχή Gateway της ενότητας Advanced features θέσαμε Gateway = OVPNDEFIANT_VPNV4, ώστε οι clients που παρατίθενται στη λίστα VPNed_hosts να περνάνε μέσα από το κρυπτογραφημένο κανάλι που υφίσταται μεταξύ pfSense και OpenVPN Access Server.



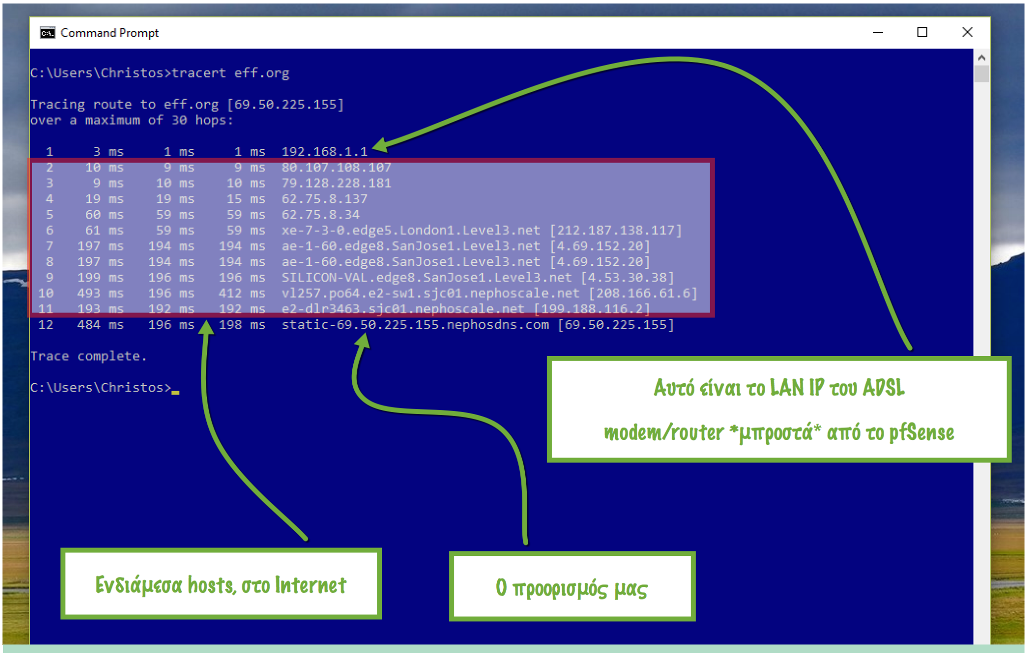
Ο τρίτος και τελευταίος κανόνας αφορά σε πακέτα που δεν προορίζονται σε κάποιον host από τη λίστα via_ISP και ταυτόχρονα δεν προέρχονται από client της λίστας VPNed_hosts. Απλά φροντίζει ώστε όλα αυτά τα πακέτα να περνάνε από το WANGW gateway, δηλαδή όχι μέσα από το κρυπτογραφημένο κανάλι.

Έλεγχοι με το mtr

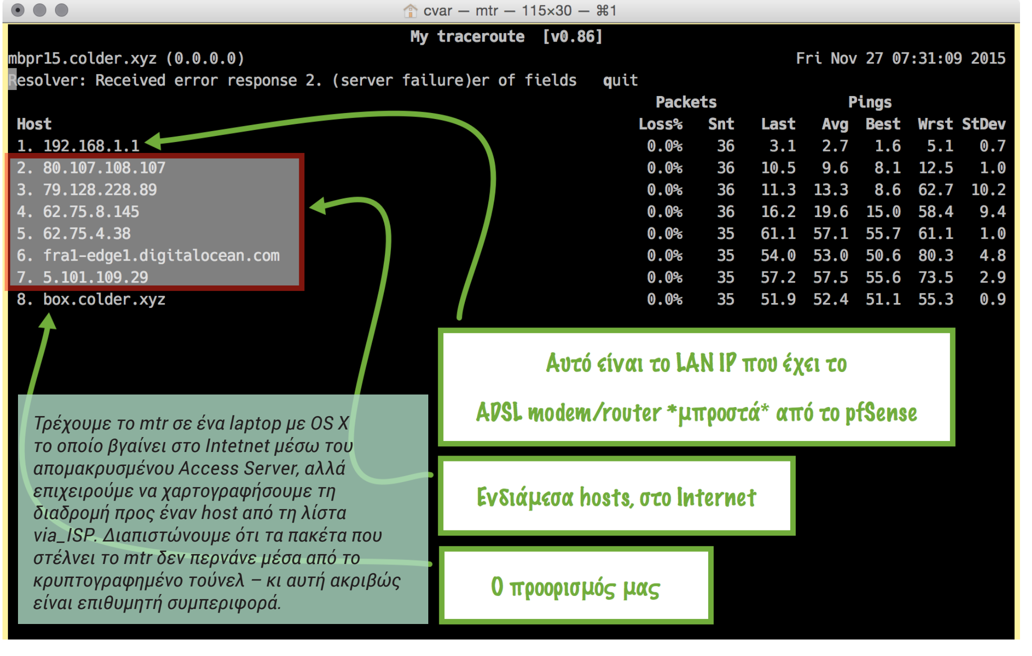
Αφού ορίσουμε τους κανόνες μας για το interface που βλέπουν οι clients του pfSense και τους εφαρμόσουμε, καλό είναι να κάνουμε και δυο-τρεις ελέγχους προκειμένου να βεβαιωθούμε ότι έχουν το επιθυμητό αποτέλεσμα. Ένα βολικό εργαλείο γι' αυτή τη δουλειά είναι το traceroute (tracert στα Windows). Εναλλακτικά υπάρχει και το mtr (http://www.bitwizard.nl/mtr), το οποίο συνδυάζει τα traceroute και ping. Τα traceroute (tracert) και mtr δείχνουν τη διαδρομή που κάνουν τα δικτυακά πακέτα από τον υπολογιστή μας έως ότου φτάσουν σε κάποιον άλλον host (στο τοπικό δίκτυο ή στο Internet). Οι έλεγχοι που εμείς κάναμε ήταν με χρήση των tracert και mtr και είχαν ως ακολούθως:

- tracert από VM με Windows 10, όπου το λειτουργικό έβγαινε στο Internet μέσω WANGW. Επιθυμητό αποτέλεσμα: Τα πακέτα *δεν* περνάνε από το κρυπτογραφημένο τούνελ.
- mtr από laptop με OS X που έβγαινε στο Internet μέσω OVPNDEFIANT_VPNV4, προς site της λίστας via_ISP. Επιθυμητό αποτέλεσμα: Τα πακέτα *δεν* περνάνε από το κρυπτογραφημένο τούνελ.
- mtr από το ίδιο laptop με OS X (και πάλι έβγαινε στο Internet μέσω OVPNDEFIANT_VPNV4), προς site *εκτός* της λίστας via_ISP. Επιθυμητό αποτέλεσμα: Τα πακέτα *περνάνε* από το κρυπτογραφημένο τούνελ.

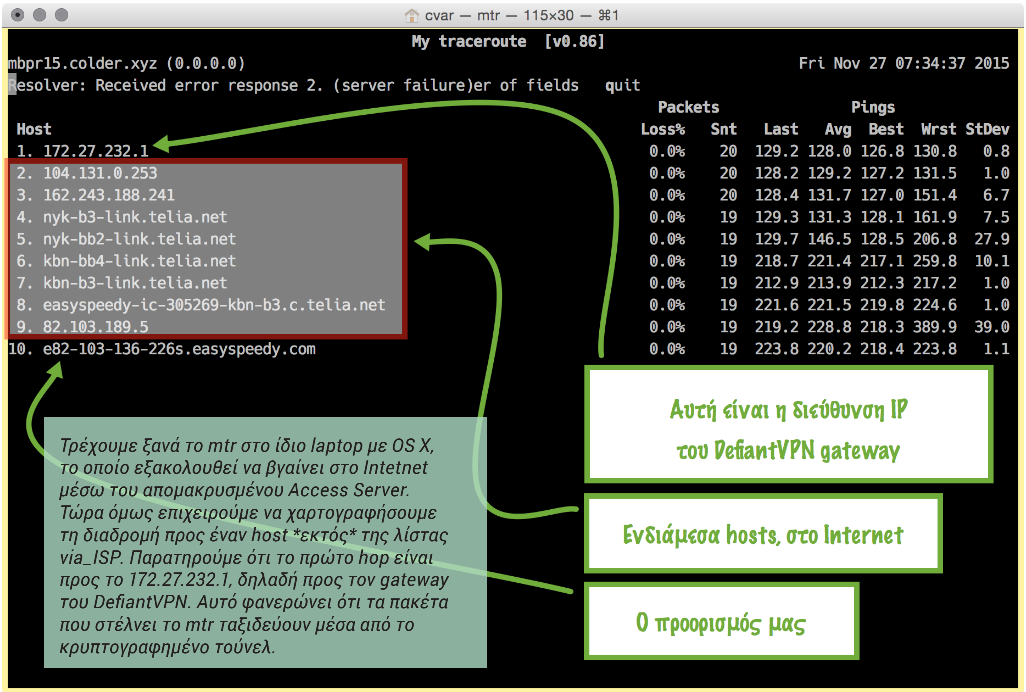
Δείτε στα screenshots που ακολουθούν μερικά στιγμιότυπα των δοκιμών μας.



*Από ένα VM με Windows 10 που *δεν* βγαίνει στο Intetnet μέσω του απομακρυσμένου OpenVPN Access Server, κάνουμε ένα tracert προς το eff.org. Το πρώτο hop είναι προς το 192.168.1.1, το οποίο είναι ο WANGW και ταυτίζεται με το LAN interface του modem/router μπροστά από το pfSense. Από εκεί και πέρα, πριν φτάσουμε στο eff.org περνάμε από 10 ενδιάμεσα μηχανήματα στο Internet. Το ότι το πρώτο hop είναι προς το 192.168.1.1 και μετά βγαίνουμε στο Internet, φανερώνει ότι η δρομολόγηση πράγματι δεν γίνεται μέσω του κρυπτογραφημένου τούνελ προς τον Access Server.*



Τρέχουμε το mtr σε ένα laptop με OS X το οποίο βγαίνει στο Intetnet μέσω του απομακρυσμένου Access Server, αλλά επιχειρούμε να χαρτογραφήσουμε τη διαδρομή προς έναν host από τη λίστα via_ISP. Διαπιστώνουμε ότι τα πακέτα που στέλνει το mtr δεν περνάνε μέσα από το κρυπτογραφημένο τούνελ – κι αυτή ακριβώς είναι επιθυμητή συμπεριφορά.

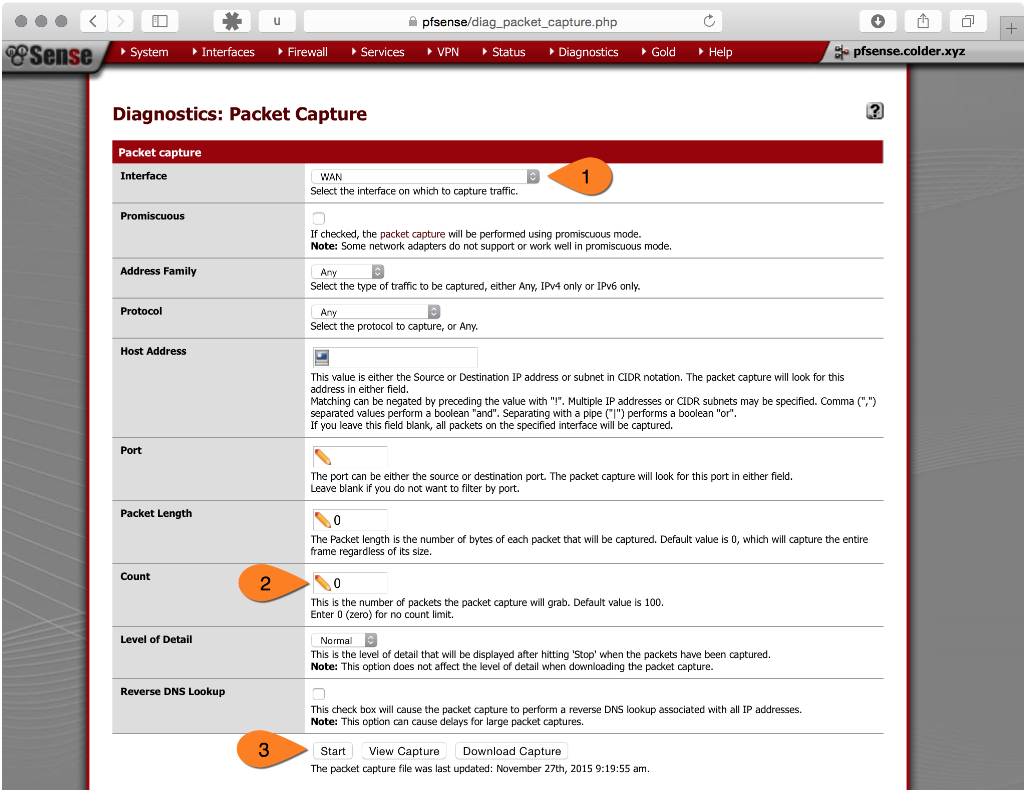


Δοκιμαστικά packet captures

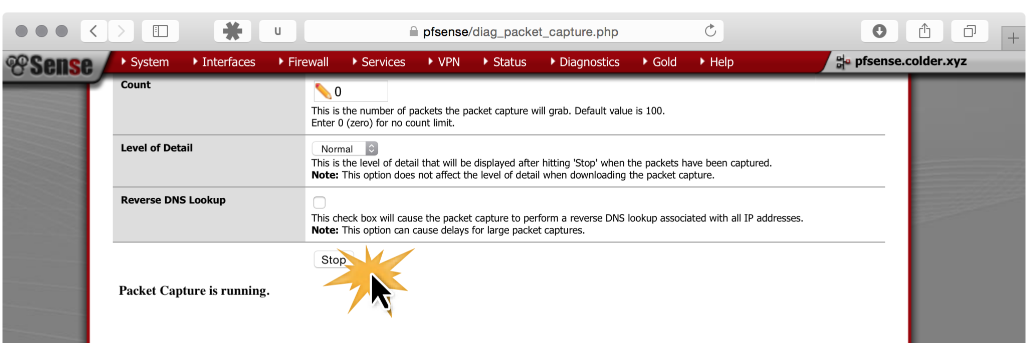
Θα ήταν διαφωτιστικό αν είχαμε μια εικόνα για το τι βλέπει ο ISP μας όταν *δεν* χρησιμοποιούμε VPN, αλλά και τι βλέπει όταν δρομολογούμε τη δικτυακή μας κίνηση *μέσω* VPN.

Κρίνοντας από τα δικά μας, φανταζόμαστε ότι ούτε για εσάς θα ‹ναι εύκολο να πάτε μια βόλτα ως το τοπικό κέντρο του ISP σας. Ακόμη κι αν πάτε, δηλαδή, κάτι μας λέει πως θα δυσκολευτείτε να πείσετε τους υπεύθυνους να συνεργαστούν και να σας αφήσουν, επιτέλους, να παρακολουθήσετε τη δική σας δικτυακή κίνηση. Δεν ξέρουμε, ίσως να κάνουμε και λάθος, θα θεωρήσουμε όμως ότι μια τέτοια απόπειρα θα αποβεί άκαρπη.

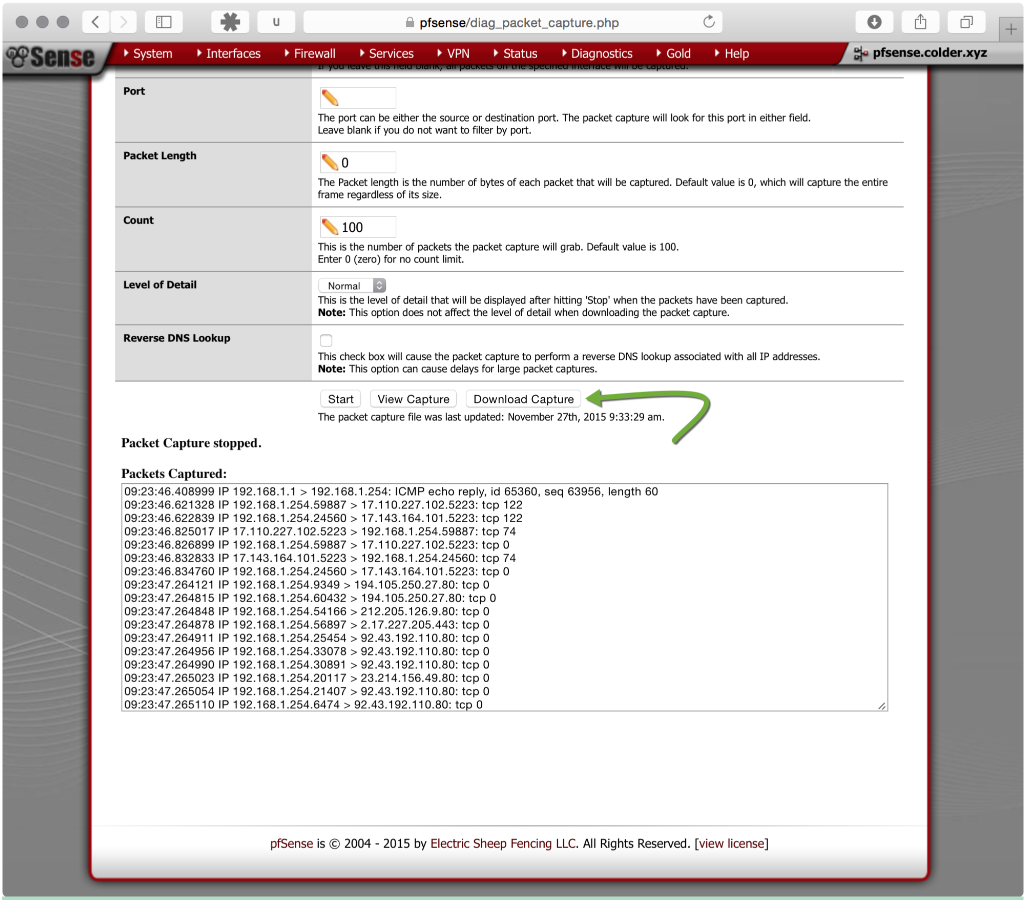
Τι μπορούμε λοιπόν να κάνουμε, αν επιθυμούμε ν' αποκτήσουμε μια εικόνα παρόμοια μ' εκείνη που έχει ο ISP μας; Μια ιδέα είναι το packet capture της δικτυακής μας κίνησης, αλλά στο επίπεδο του pfSense. Πιο συγκεκριμένα, προτείνουμε δύο captures: ένα όταν έχουμε δικτυακή κίνηση που δεν δρομολογείται μέσω Access Server, βεβαίως κι άλλο ένα όταν έχουμε δικτυακή κίνηση που δρομολογείται μέσω Access Server. Θα πάρουμε έτσι δύο διαφορετικά αρχεία και, στη συνέχεια, με την ησυχία μας θα επιχειρήσουμε μια κάποια ανάλυση, καταφεύγοντας σε εργαλεία όπως το tcpdump ή το Wireshark. Δείτε στα screenshots που ακολουθούν πώς πετυχαίνουμε το packet capture με χρήση της σχετικής δυνατότητας που παρέχει το ίδιο το pfSense.



Για ένα packet capture μέσα από το περιβάλλον του pfSense, απλά ακολουθούμε τη διαδρομή Diagnostics Packet Capture. Θέλουμε να συλλάβουμε πακέτα που διέρχονται από το interface ονόματι WAN, γι' αυτό και θέτουμε Interface = WAN (1). Δεν επιλέγουμε το DefiantVPN, αφού τη στιγμή που τα πακέτα εισέρχονται σ' αυτό το interface δεν είναι ακόμη κρυπτογραφημένα. Βγαίνοντας όμως από το WAN, αν προηγουμένως είχαν περάσει από το DefiantVPN τότε θα είναι κρυπτογραφημένα. Για τις παραμέτρους Address Family, Protocol, Host Address, Port και Packet Length αφήνουμε τις προεπιλεγμένες τιμές, αφού το packet capture επιθυμούμε να είναι όσο πιο γενικό γίνεται. Θέτοντας Count = 0 (2) το packet capture θα παραμένει ενεργό έως ότου αποφασίσουμε να το σταματήσουμε εμείς οι ίδιοι. Προκειμένου να ξεκινήσει η διαδικασία, ένα κλικ στο κουμπάκι Start (3) είναι αρκετό.



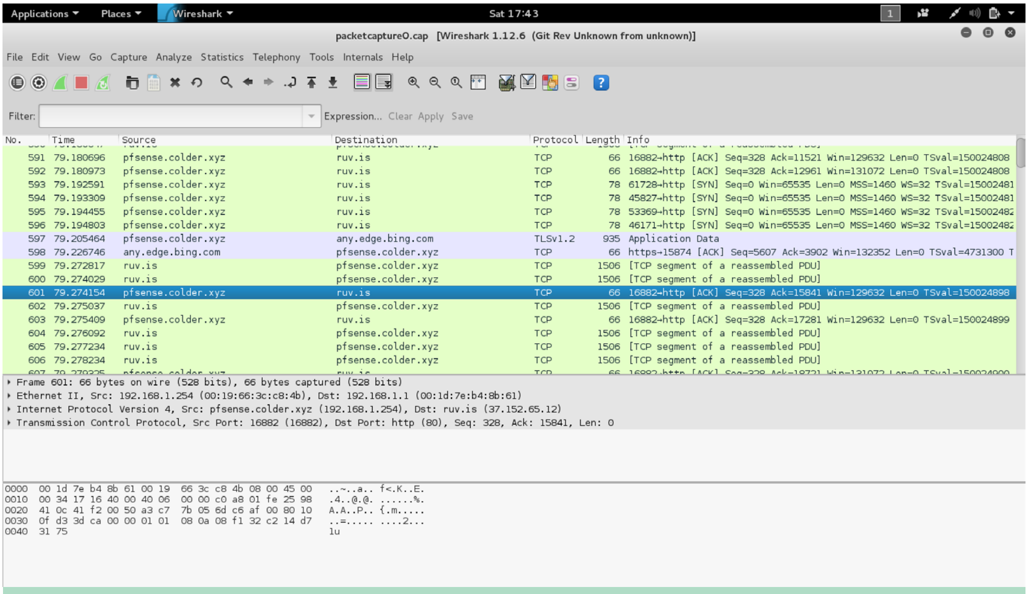
Όση ώρα λαμβάνει χώρα ένα packet capture, στο κάτω μέρος της σελίδας Diagnostics Packet Capture εμφανίζεται το λακωνικό μήνυμα "Packet Capture is running.". Όταν αοφασίσουμε να το σταματήσουμε, απλά θα κάνουμε ένα κλικ στο κουμπάκι Stop.



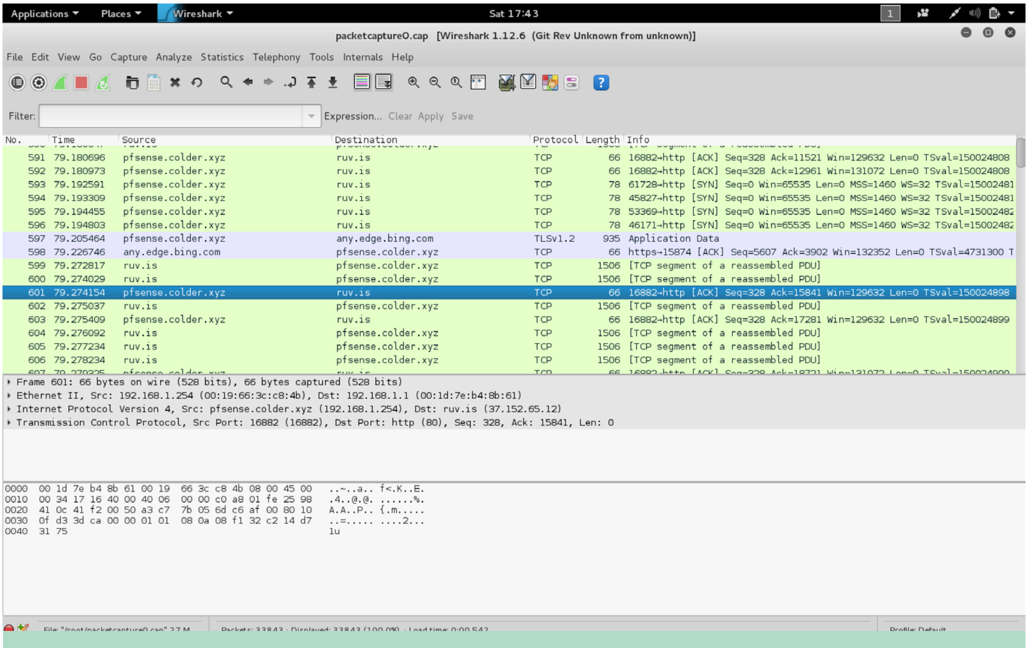
Αφού σταματήσουμε ένα packet capture, αναλόγως του όγκου των δεδομένων που καταγράφηκαν ίσως χρειαστεί να περιμένουμε μερικά λεπτά. Τελικά, με κλικ στο κουμπί Download Capture θα αποθηκεύσουμε στον υπολογιστή μας ένα αρχείο με κατάληξη .cap, το οποίο θα περιμβάνει όλα τα δικτυακά πακέτα που αποθηκεύτηκαν κατά το προηγούμενο session.

Εξέταση/ανάλυση των packet captures

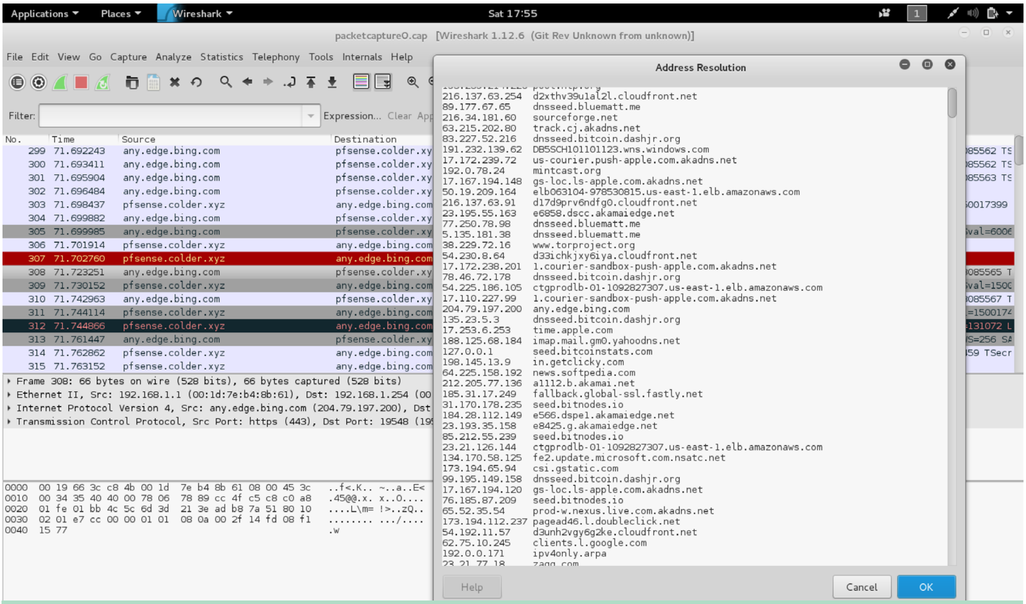
Μετά τα packet captures, τα αρχεία .cap που έχουμε στη διάθεσή μας μπορούμε να τα αναλύσουμε με ένα εργαλείο σαν το tcpdump ή με μια εφαρμογή όπως το Wireshark. Για το packet analysis γενικότερα διαβάστε τα σχετικά άρθρα που δημοσιεύονται στα τεύχη 019 και 020 του deltaHacker. Σ' αυτά θα βρείτε και συγκεκριμένα παραδείγματα ανάλυσης. Στα screenshots που ακολουθούν βλέπουμε μερικά πρώτα συμπεράσματα που προέκυψαν άμεσα με τη βοήθεια του Wireshark, μετά από δύο packet captures που κάναμε στο δικό μας pfSense box.



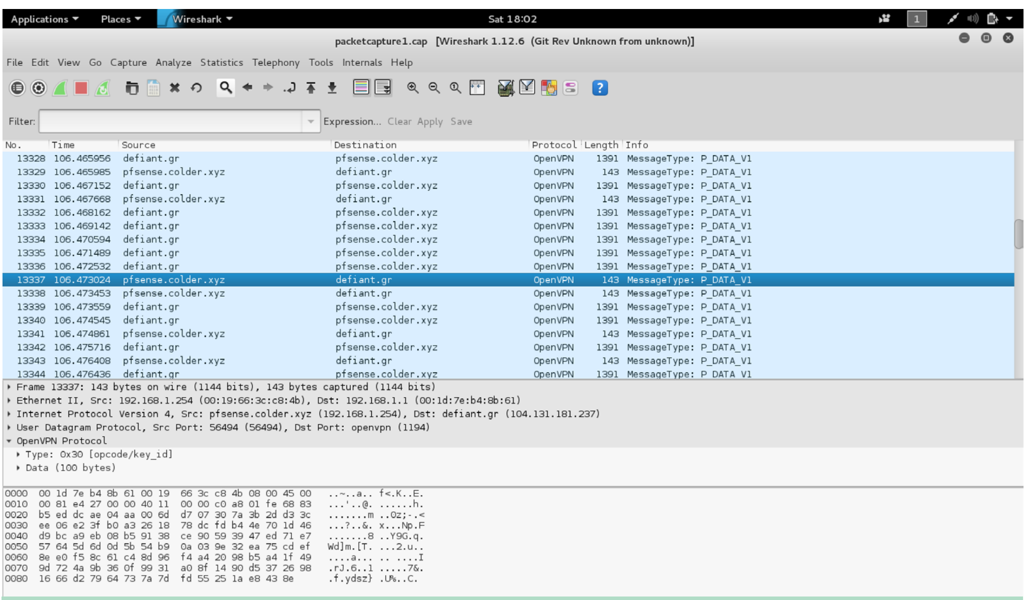
Έχουμε φορτώσει στο Wireshark το αρχείο ονόματι packetcapture0.cap, το οποίο δημιουργήθηκε όταν κανένας client δεν χρησιμοποιούσε τον απομακρυσμένο OpenVPN Access Server. Πολύ γρήγορα διαπιστώνουμε ότι οι δραστηριότητες των χρηστών αποκαλύπτονται εύκολα. Στο στιγμιότυπο διακρίνουμε μέρος της επικοινωνίας μεταξύ του router (pfsense.colder.xyz) και του ruv.is – Κύριος οίδε γιατί!



Ιδού μερικές από τις συνδέσεις που έλαβαν χώρα μεταξύ του pfSense router και απομακρυσμένων hosts. (Κάποιος έχει αρχίσει να παίζει με το Bitcoin ή είναι η ιδέα μας;)



Μερικές από τις διευθύνσεις IP και τα αντίστοιχα fully qualified domain names των ιντερνετικών hosts, με τους οποίους επικοινώνησε ο router μας κατά τη διάρκεια του packet capture. Σ' αυτό το μέρος της λίστας δεν φαίνεται να υπάρχει τίποτε άτακτο. Για λίγο πιο πάνω ή για λίγο πιο κάτω, δεν βάζουμε το χέρι μας στη φωτιά.



Εδώ έχουμε ανοίξει το αρχείο packetcapture1.cap, το οποίο δημιουργήθηκε όταν στο τοπικό δίκτυο λειτουργούσαν μόνο clients τους οποίους ο router έβγαζε έξω αποκλειστικά μέσω Access Server. Παρατηρούμε ότι υπάρχει έντονη επικοινωνία μεταξύ pfsense.colder.xyz και defiant.gr. Παρεμπιπτόντως, αυτό το τελευταίο είναι το FQDN του VPS στο οποίο λειτουργεί ο VPN server. Το πρωτόκολλο επικοινωνίας μεταξύ των δύο μηχανημάτων είναι αναγνωρίσιμο (βλ. στήλη Protocol), ωστόσο το περιεχόμενο της επικοινωνίας είναι ισχυρά κρυπτογραφημένο και καμία άλλη χρήσιμη πληροφορία δεν μπορεί να προκύψει.

Skill: Beginner
Tags: EncFS, cloud storage, Linux, Windows

Έξτρα κρυπτογράφηση για τα δεδομένα μας στο cloud

Η τάση που θέλει τα πάντα να βρίσκονται online εγείρει σημαντικά ζητήματα ασφαλείας. Πόσο προσωπικά θα είναι τα προσωπικά μας δεδομένα, αν τα αποθηκεύσουμε στους servers κάποιας εταιρείας; Όλες όσες προσφέρουν το λεγόμενο cloud storage διατείνονται πως μόνον εμείς έχουμε πρόσβαση στα δεδομένα μας και, εδώ που τα λέμε, δεν θα μπορούσαν να ισχυριστούν κάτι διαφορετικό. Για άλλη μια φορά, όσοι παίρνουν στα σοβαρά την ασφάλεια των δεδομένων τους, πρέπει να πάρουν και τα μέτρα τους.

του Πέτρου Κυλαδίτη

Η ευκολία που προσφέρει το Dropbox και όλες οι παρόμοιες υπηρεσίες είναι τόσο μεγάλη, που πολύ συχνά θυσιάζουμε την ασφάλεια των δεδομένων μας χωρίς δεύτερη σκέψη. Μήπως πρέπει να αναθεωρήσουμε αυτού του είδους τις συνήθειες; Ακόμα κι αν δεχτούμε ως αληθείς τις υποσχέσεις που δίνουν οι εταιρείες του χώρου, κανένας δεν εγγυάται ότι διαθέτουν άτρωτα συστήματα. Μπορεί όταν κάνουν λόγο για ασφάλεια και διακριτικότητα να το εννοούν, αλλά αν πέσουν θύματα μιας επίθεσης τα δεδομένα μας πιθανώς θα εκτεθούν. Μια προφανής λύση, ώστε να μην καταντήσουμε να αφορίσουμε την τεχνολογία και τις ευκολίες που προσφέρει, είναι να στραφούμε σε κάποια μέθοδο κρυπτογράφησης *πριν* το ανέβασμα των δεδομένων στο cloud. Ποια είναι η καταλληλότερη, όμως;

Εμφωλευμένη κρυπτογράφηση

Κρυπτογράφηση προσφέρουν όλες οι υπηρεσίες που παρέχουν λύσεις cloud storage, ωστόσο στην πλειονότητα των περιπτώσεων κατέχουν και τα κλειδιά της αποκρυπτογράφησης. Ακριβώς γι' αυτό ενδιαφερόμαστε για ένα πρόσθετο στάδιο κρυπτογράφησης, το οποίο θα ελέγχουμε αποκλειστικά εμείς. Με άλλα λόγια, τα δεδομένα που θα συγχρονίζουμε μεταξύ του υπολογιστή μας και των servers της εκάστοτε εταιρείας θα είναι ήδη κρυπτογραφημένα – και το κλειδί της αποκρυπτογράφησης θα το κατέχουμε εμείς και μόνον εμείς.

Για να πετύχουμε κάτι τέτοιο, μια πρώτη λύση που έρχεται στο μυαλό είναι το VeraCrypt. Πρόκειται για ένα εργαλείο που προσφέρει όλες τις λειτουργίες του πάλαι ποτέ TrueCrypt, ενώ διορθώνει κι όλες τις αδυναμίες που είχαν εντοπιστεί στο προαναφερθέν. Η συγκεκριμένη λύση, αν και είναι αρκετά ισχυρή και μπορεί να εφαρμοστεί σε πολλές πλατφόρμες, παρουσιάζει ένα σημαντικό μειονέκτημα: Το VeraCrypt δημιουργεί κρυπτογραφημένους τόμους, αλλά δεν μπορεί να κρυπτογραφεί μεμονωμένα αρχεία. Αν δημιουργήσουμε έναν τέτοιο τόμο για την ασφαλή αποθήκευση των δεδομένων μας, προκειμένου να έχουμε πρόσβαση στα αρχεία μας μέσω κάποιας υπηρεσίας cloud storage θα πρέπει να συγχρονίζουμε ολόκληρο τον τόμο! Μάλιστα, εξαιτίας της φύσης των κρυπτογραφημένων δεδομένων, κάθε φορά που θα τροποποιούμε ένα αρχείο εντός του κρυπτογραφημένου τόμου, θα πρέπει να το ανεβάζουμε ολόκληρο στο cloud εκ νέου.

Γίνεται λοιπόν φανερό ότι η λύση της κρυπτογράφησης ενός δίσκου, ενός διαμερίσματος ή ενός εικονικού τόμου, ναι μεν αυξάνει την ασφάλεια αλλά περιορίζει δραστικά την ευκολία όσον αφορά στο cloud. Υπάρχουν εξάλλου πολλές μέθοδοι για την κρυπτογράφηση ολόκληρων συστημάτων αρχείων, αλλά κανένα δεν εξυπηρετεί ως προς τη συνεργασία με το cloud storage.

Ευτυχώς, αυτό το κενό ανάμεσα στην αυξημένη ασφάλεια και στην ευκολία, μπορεί να το καλύψει το EncFS. Αν και τ' όνομά του παραπέμπει στη δημιουργία ενός κρυπτογραφημένου συστήματος αρχείων, η συμπεριφορά του δεν έχει καμία σχέση με τις λύσεις που αναφέραμε μόλις. Το EncFS στηρίζεται στους υπάρχοντες τόμους του υπολογιστή μας και, χωρίς να δημιουργεί κάποιο εξειδικευμένο σύστημα αρχείων, καταφέρνει να κρυπτογραφεί όσα και όποια αρχεία θέλουμε. Με άλλα λόγια, αποτελεί έναν μηχανισμό κρυπτογράφησης και αποκρυπτογράφησης αρχείων ο οποίος τηρεί τα κρυπτογραφημένα δεδομένα στην υπάρχουσα υποδομή (τόμους και συστήματα αρχείων). Έτσι, αντί να έχουμε ένα ογκώδες κρυπτογραφημένο αρχείο με όλα τα δεδομένα μας (λύση τύπου VeraCrypt), διαθέτουμε πολλά και μικρά κρυπτογραφημένα αρχεία. Αυτή η προσέγγιση επιτρέπει τον γρήγορο συγχρονισμό των δεδομένων μας και δεν περιορίζει καθόλου την ευχρηστία που παρέχουν οι υπηρεσίες cloud storage. Παρεμπιπτόντως, αυξημένη ταχύτητα έχουμε και κατά τη χρήση των κρυπτογραφημένων δεδομένων, αφού ο υπολογιστής αποκρυπτογραφεί κάθε φορά ένα μόνο αρχείο κι όχι έναν ολόκληρο τόμο.

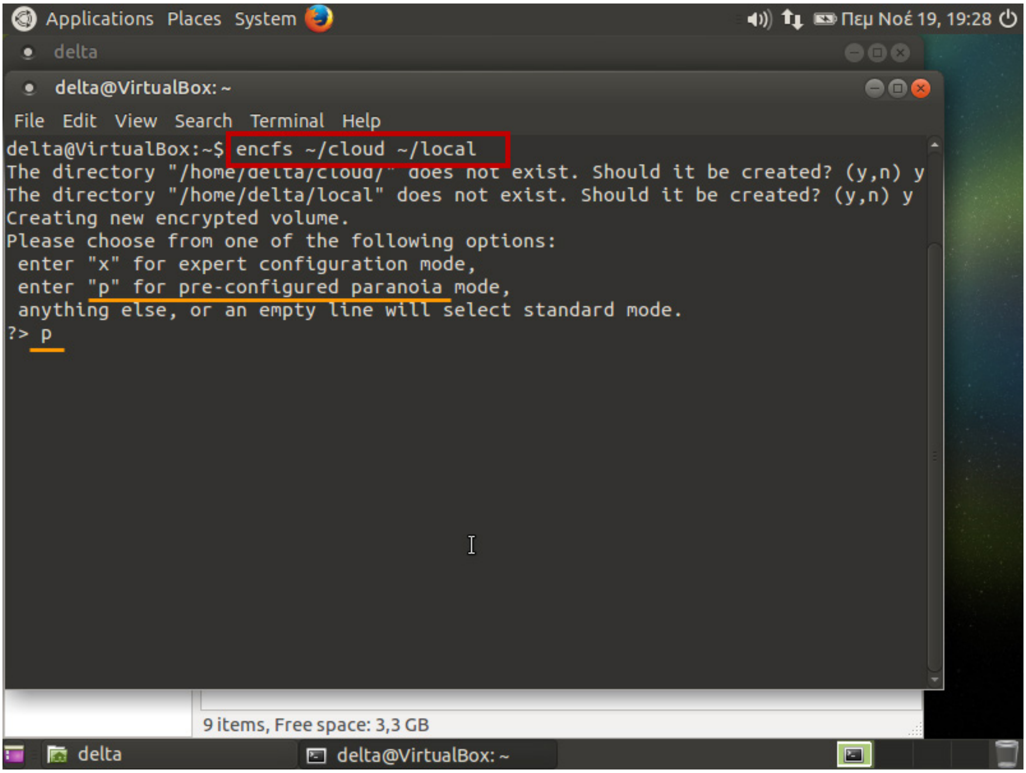
Στα ενδότερα

Η λειτουργία του EncFS δεν είναι πολύπλοκη. Ο χρήστης πρέπει να επιλέξει ένα κλειδί κρυπτογράφησης, καθώς και δύο τοποθεσίες εντός των αποθηκευτικών του μέσων. Στη μία θέση αποθηκεύονται τα κρυπτογραφημένα αρχεία, ενώ στην άλλη εμφανίζονται τα αρχεία στην πρωτότυπη/μη-κρυπτογραφημένη μορφή. Παρατηρήστε ότι μιλάμε για εμφάνιση των πρωτότυπων αρχείων και όχι για αποθήκευση, διατήρηση ή κάτι τέτοιο. Στο δίσκο αποθηκεύεται *μόνο* η κρυπτογραφημένη εκδοχή των αρχείων. Η μη-κρυπτογραφημένη εκδοχή παράγεται δυναμικά από το EncFS κι εμφανίζεται στη δεύτερη τοποθεσία, χωρίς να βρίσκεται πραγματικά εκεί. Ουσιαστικά, η δεύτερη τοποθεσία αποτελεί το σημείο προσάρτησης (mount point) ενός εικονικού συστήματος αρχείων, το οποίο περιλαμβάνει τα μη-κρυπτογραφημένα

δεδομένα. Ως εκ τούτου, στην περίπτωση που διακοπεί η λειτουργία του EncFS, το εικονικό σύστημα αρχείων παύει να υφίσταται, αποπροσαρτάται αυτόματα και τα μη-κρυπτογραφημένα αρχεία παύουν να είναι διαθέσιμα. Όπως αντιλαμβάνεστε, οι δύο θέσεις που αναφέραμε προσδιορίζονται από δύο καταλόγους. Ο πρώτος, αυτός με τα κρυπτογραφημένα δεδομένα, πρέπει να βρίσκεται εντός του καταλόγου που συγχρονίζεται με την υπηρεσία cloud storage. Αντίθετα, ο δεύτερος πρέπει να βρίσκεται σε κάποια άλλη, ασφαλέστερη θέση. Κατ' αυτόν τον τρόπο, τα αρχεία μας θα ταξιδεύουν στο δίκτυο και θα αποθηκεύονται στους servers της εκάστοτε εταιρείας όντας κρυπτογραφημένα δύο φόρες (μία από το EncFS και μία από το software της εταιρείας cloud storage). Φυσικά, για το πρώτο επίπεδο κρυπτογράφησης έχουμε τον αποκλειστικό έλεγχο των κλειδιών αποκρυπτογράφης εμείς και κανείς άλλος.

Οι πιο δύσπιστοι αναγνώστες μπορεί να σκέφτονται ήδη ότι όλο και κάπου θα κρύβεται κάποια παγίδα. Η λύση που περιγράψαμε είναι αρκετά απλή για να είναι εύχρηστη και ταυτόχρονα ασφαλής. Για την ευχρηστία πιστεύουμε ότι θα σας πείσουμε στη συνέχεια του άρθρου. Σε σχέση με την ασφάλεια, όμως, πρέπει να σας πούμε ότι δεν είσαστε οι μόνοι που ανησυχείτε. Ο ερευνητής Taylor Hornby έχει εντοπίσει αρκετά σημεία που δεν του αρέσουν στο EncFS, το κυριότερο από τα οποία σχετίζεται με την προεπιλεγμένη θέση αποθήκευσης των ρυθμίσεων. Το σχετικό αρχείο αποθηκεύεται στον κατάλογο με τα κρυπτογραφημένα αρχεία και περιλαμβάνει τη μέθοδο κρυπτογράφησης που επέλεξε ο χρήστης, το δημόσιο κλειδί κ.ά. Σύμφωνα με τον ερευνητή, αν κάποιος επιτιθέμενος διαβάσει το αρχείο ρυθμίσεων κι αποκτήσει δύο ή περισσότερα στιγμιότυπα (snapshots) των κρυπτογραφημένων αρχείων, υπάρχει η *πιθανότητα* να πετύχει την αποκρυπτογράφηση των δεδομένων. Μέχρι σήμερα δεν έχει παρουσιαστεί κάποια απτή μέθοδος εκμετάλλευσης αυτής της αδυναμίας, αλλά ο θεωρητικός κίνδυνος παραμένει. Όπως έχουμε πει αρκετές φορές, η ευκολία έρχεται μ' ένα τίμημα. Αυτή τη φορά τουλάχιστον το τίμημα είναι μικρό, καθώς μιλάμε για έναν θεωρητικό κίνδυνο. Εξάλλου, πρέπει να λάβουμε υπόψη ότι δεν εξετάζουμε τη συγκρότηση του δικού μας συστήματος συγχρονισμού και αποθήκευσης αρχείων. Ο σκοπός μας είναι να αυξήσουμε την ασφάλεια που παρέχει μια υπάρχουσα υπηρεσία του είδους και χωρίς αμφιβολία τον πετυχαίνουμε. Σκεφτείτε ότι αν η πιθανότητα του να "σπάσει" κανείς την κρυπτογράφηση του EncFS είναι πολύ μικρή, η δεσμευμένη πιθανότητα του να σπάσει αυτή την κρυπτογράφηση καθώς κι εκείνη που χρησιμοποιείται από την υπηρεσία του cloud storage είναι *εξαιρετικά* μικρή. Ακολουθώντας αυτό το σκεπτικό συμπεραίνουμε ότι μπορούμε να χρησιμοποιήσουμε το EncFS άφοβα, αλλά χωρίς να αγνοούμε εντελώς την έρευνα του αγαπητού Hornby.

Στη συνέχεια θα δούμε πώς μπορούμε να προφυλάσσουμε ακόμα περισσότερο τα αρχεία που συγχρονίζουμε μέσω Dropbox, δουλεύοντας τόσο σε Linux όσο και σε Windows.



Στιγμιότυπο από την πρώτη εκτέλεση του EncFS στο δικό μας σύστημα. Επειδή οι κατάλογοι cloud και local δεν υπήρχαν, το πρόγραμμα προσφέρθηκε να τους δημιουργήσει. Στη συνέχεια ερωτηθήκαμε για τον τρόπο ρύθμισης του προγράμματος και προτιμήσαμε τον προεπιλεγμένο, με τον χαρακτηρισμό "paranoia".

Εργασία στο Linux

Το EncFS αναπτύχθηκε για το Linux και η λειτουργία του στηρίζεται στο γνωστό kernel module ονόματι FUSE. Το εν λόγω άρθρωμα και η ομώνυμη βιβλιοθήκη αξιοποιούν τη σχετική υποδομή του πυρήνα και επιτρέπουν σε απλά προγράμματα να δημιουργούν και να χειρίζονται ολόκληρα file systems. Εμείς εργαστήκαμε σε μια διανομή που βασίζεται στο Debian (Ubundu Mate) κι εγκαταστήσαμε το EncFS από τα repositories της διανομής:

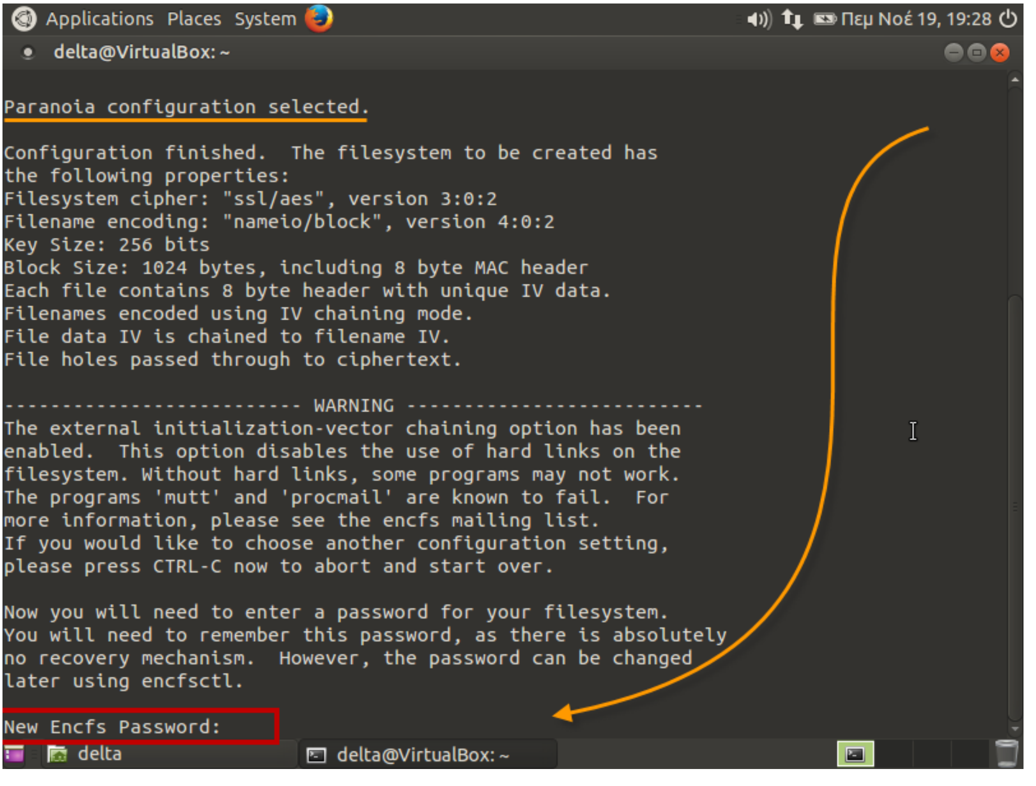
```
sudo apt-get install encfs
```

Η εγκατάσταση περιλαμβάνει τη λήψη κάποιων πρόσθετων αρχείων, καθώς και μια σύντομη ενημέρωση για τα αποτελέσματα της έρευνας του Hornby. Στα σχετικά ερωτήματα απαντάμε θετικά, η εγκατάσταση ολοκληρώνεται πολύ γρήγορα και το EncFS είναι έτοιμο προς χρήση. Αν και υπάρχουν αρκετά GUIs για το χειρισμό του επιλέξαμε να δουλέψουμε από τη γραμμή εντολών, που επιτρέπει και την πλήρη παραμετροποίηση του προγράμματος.

Ας υποθέσουμε ότι μέσα στο home directory του χρήστη μας υπάρχουν οι κατάλογοι cloud και local. Ο πρώτος συγχρονίζεται μεταξύ διαφόρων υπολογιστών με τη βοήθεια του Dropbox, ενώ ο δεύτερος είναι εκείνος από τον οποίο θέλουμε να αποκτάμε πρόσβαση στα κρυπτογραφημένα αρχεία. Ο πιο απλός τρόπος χρήσης του EncFS έχει ως εξής:

```
encfs ~/cloud ~/local
```

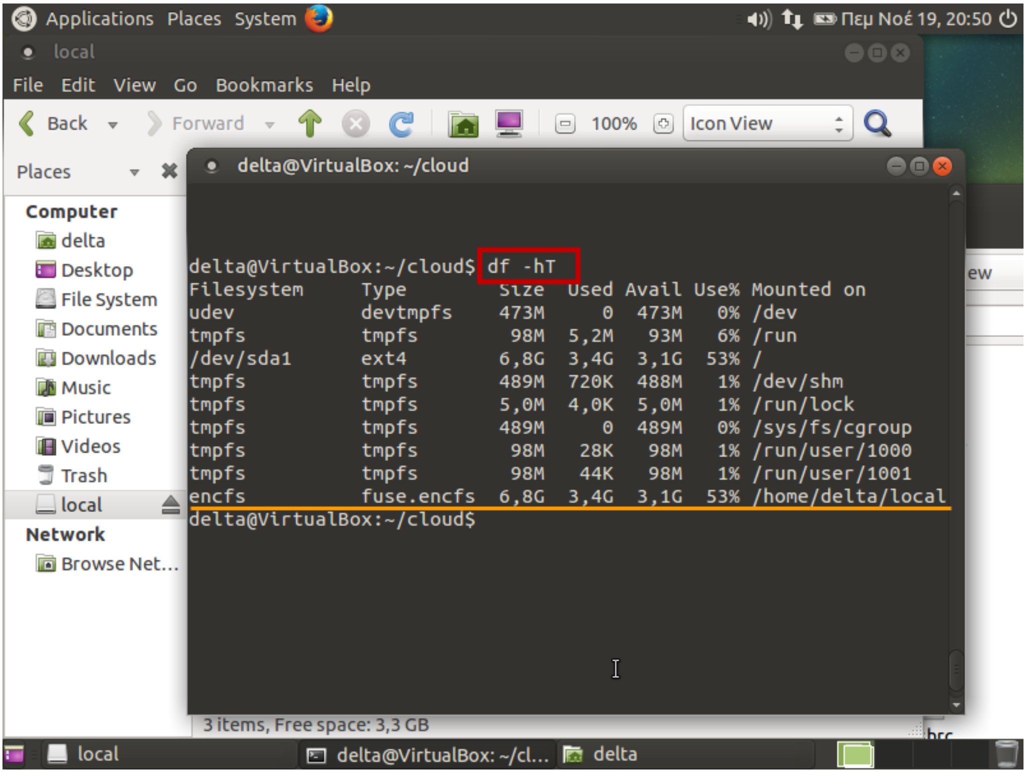
Σημειώστε ότι αν οι κατάλογοι cloud και local δεν υπήρχαν, το πρόγραμμα δεν θα διαμαρτυρόταν κι απλά θα μας ρωτούσε αν επιθυμούμε τη δημιουργία τους. Εκτελώντας την παραπάνω γραμμή, το EncFS θα μας απευθύνει μια σειρά ερωτήσεων σχετικά με τους αλγόριθμους κρυπτογράφησης που θέλουμε να χρησιμοποιεί. Οι προεπιλεγμένες (παρανοϊκές) ρυθμίσεις προσφέρουν ικανοποιητική ασφάλεια. Αμέσως μετά, το πρόγραμμα ζητά να ορίσουμε έναν κωδικό πρόσβασης, τον οποίο θα πρέπει να δίνουμε για την αποκρυπτογράφηση των αρχείων. Αυτό ήταν όλο.



Αμέσως μετά την επιλογή των επιθυμητών ρυθμίσεων, καλούμαστε να ορίσουμε τον κωδικό για το κλείδωμα των αρχείων μας.

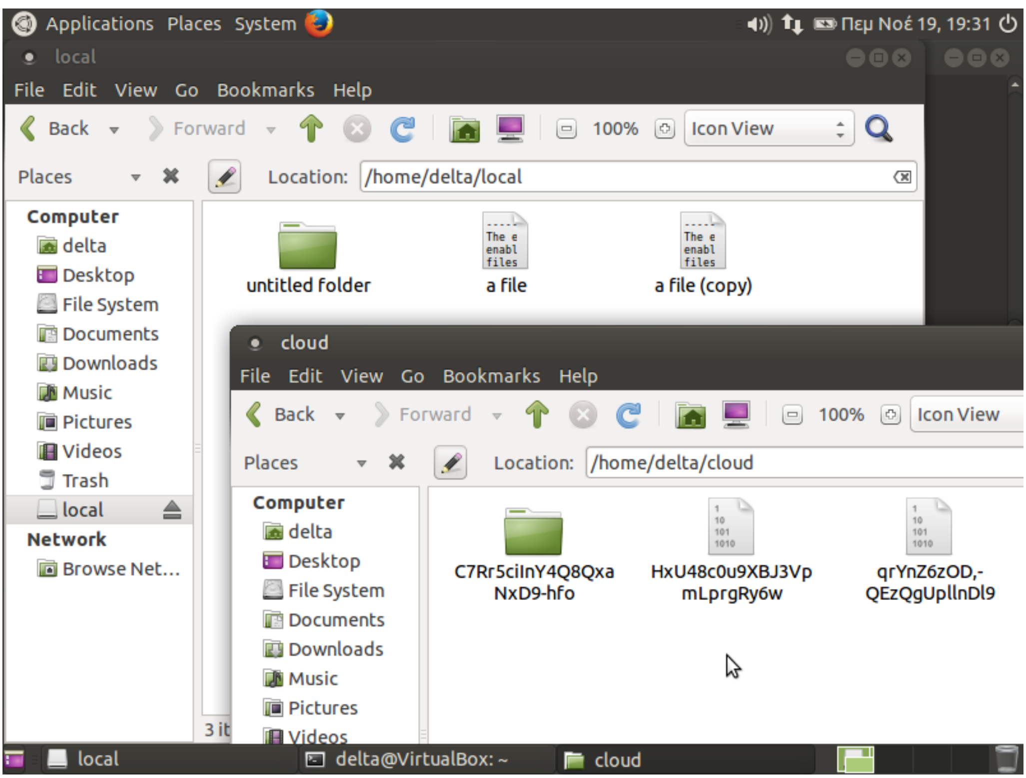
Αν τσεκάρουμε τα προσαρτημένα συστήματα αρχείων με τη βοήθεια του εργαλείου df, θα διαπιστώσουμε ότι στον κατάλογο ~/local έχει προσαρτηθεί ένα νέο file system του τύπου fuse.encfs. Πλέον, αν τοποθετήσουμε κάποιο αρχείο εντός του local, το περιεχόμενο του αρχείου θα κρυπτογραφηθεί αυτόματα και θα αποθηκευτεί στον κατάλογο ~/cloud, με ένα επίσης κρυπτογραφημένο όνομα. Στον ίδιο τον κατάλογο local δεν θα αποθηκευτεί απολύτως τίποτα. Για του λόγου το αληθές, μπορείτε να κάνετε ένα μικρό πείραμα. Αφού αποπροσαρτήσετε τον εν λόγω κατάλογο, επιστρατεύστε όσα προγράμματα ανάκτησης δεδομένων θέλετε. Να είσαστε σίγουροι ότι δεν πρόκειται να βρείτε τίποτα, αφού το EncFS φροντίζει να γράφει μόνο την κρυπτογραφημένη εκδοχή των δεδομένων και μόνο στον κατάλογο cloud. Τα αρχεία σε μη-κρυπτογραφημένη μορφή δεν αποθηκεύονται πουθενά! Παρεμπιπτόντως, όπως συμβαίνει με πολλά συστήματα αρχείων που στηρίζονται στο FUSE, για την αποπροσάρτηση του local μπορούμε να χρησιμοποιήσουμε το εργαλείο fusermount κάπως έτσι:

```
fusermount -u ~/local
```



Αν ρίξουμε μια ματιά στα προσαρτημένα συστήματα αρχείων, θα δούμε ότι το EncFS δημιούργησε έναν εικονικό τόμο και τον προσάρτησε στον κατάλογο local.

Αν προσπαθήσουμε να ξεκινήσουμε ξανά το EncFS, δηλώνοντας ως προορισμό για τα κρυπτογραφημένα αρχεία τον ίδιο κατάλογο (cloud), το πρόγραμμα δεν θα εμφανίσει τις ερωτήσεις που αναφέραμε προηγουμένως. Θα ζητήσει μόνο τον κωδικό για την αποκρυπτογράφηση. Βλέπετε, στον κατάλογο με τα κρυπτογραφημένα αρχεία αποθηκεύονται και όλες οι ρυθμίσεις του προγράμματος. Το σχετικό αρχείο (.encfs6.xml) είναι εξέχουσας σημασίας. Αν χαθεί θα χαθούν μαζί και τα δεδομένα μας, αφού η αποκρυπτογράφησή τους θα είναι πλέον αδύνατη. Όπως αναφέραμε εισαγωγικά, η θέση αποθήκευσης αυτού του αρχείου ήταν ένα από τα στοιχεία που ανησύχησαν ιδιαίτερα τον ερευνητή Taylor Hornby. Έτσι, σε μια προσπάθεια να περιορίσουμε τις πιθανότητες "σπασίματος" της κρυπτογράφησης του EncFS, θα δούμε πώς μπορούμε να αλλάξουμε τη θέση του.



Όταν εργαζόμαστε στο φάκελο που παρέχει πρόσβαση στα μη-κρυπτογραφημένα αρχεία, είναι δύσκολο να φανταστούμε το μπάχαλο που μοιάζει να επικρατεί στον πραγματικό φάκελο αποθήκευσης των αρχείων. Το EncFS φροντίζει να κρυπτογραφεί τόσο το περιεχόμενο των αρχείων, όσο και τα ονόματά τους.

Αποφασίσαμε να αποθηκεύσουμε το αρχείο ρυθμίσεων του EncFS στο home directory του χρήστη μας. Όπως αντιλαμβάνεστε δεν πρόκειται για την πιο ασφαλή τοποθεσία, αλλά είναι σίγουρα προτιμότερη από τον κατάλογο cloud, που συγχρονίζεται με το Dropbox. Όποια επιλογή κι αν κάνετε εσείς για την αποθήκευση του αρχείου ρυθμίσεων, πρέπει να ενημερώσετε και το EncFS κατά την εκκίνησή του. Αυτό δεν γίνεται με τη βοήθεια κάποιας παραμέτρου, αλλά με τη χρήση μιας μεταβλητής περιβάλλοντος που έχει το όνομα ENCFS6_CONFIG. Στη δική μας περίπτωση, για να ξεκινήσουμε το EncFS πληκτρολογούμε

```
export ENCFS6_CONFIG=~/.encfs6.xml
```

και μετά

```
encfs ~/cloud ~/local
```

Σε αυτό το σημείο μπορεί να προβληματιστείτε. Υποτίθεται ότι επιλέξαμε το EncFS επειδή θα αύξανε την ασφάλεια χωρίς να μας παιδέψει. Ωστόσο, ο ορισμός μιας μεταβλητής περιβάλλοντος πριν από την εκτέλεση, έστω κι αν πραγματοποιείται μόνο μία φορά σε κάθε επανεκκίνηση του υπολογιστή, ίσως θεωρηθεί κάπως μπελαλίδικη. Μια καλή ιδέα θα ήταν η δημιουργία ενός μικροσκοπικού BASH script, που θα ορίζει τη μεταβλητή ENCFS6_CONFIG και στη συνέχεια θα εκτελεί το EncFS με τις κατάλληλες παραμέτρους. Εμείς φτιάξαμε το σχετικό script και του δώσαμε το όνομα cloud_unlock.sh. Επειδή μάς αρέσουν η κομψότητα και η συμμετρία, δημιουργήσαμε κι ένα script με το όνομα cloud_lock.sh. Αυτό το δεύτερο script αξιοποιεί το fusermount κι αποσυνδέει τον κατάλογο που παρέχει πρόσβαση στα αποκρυπτογραφημένα αρχεία.

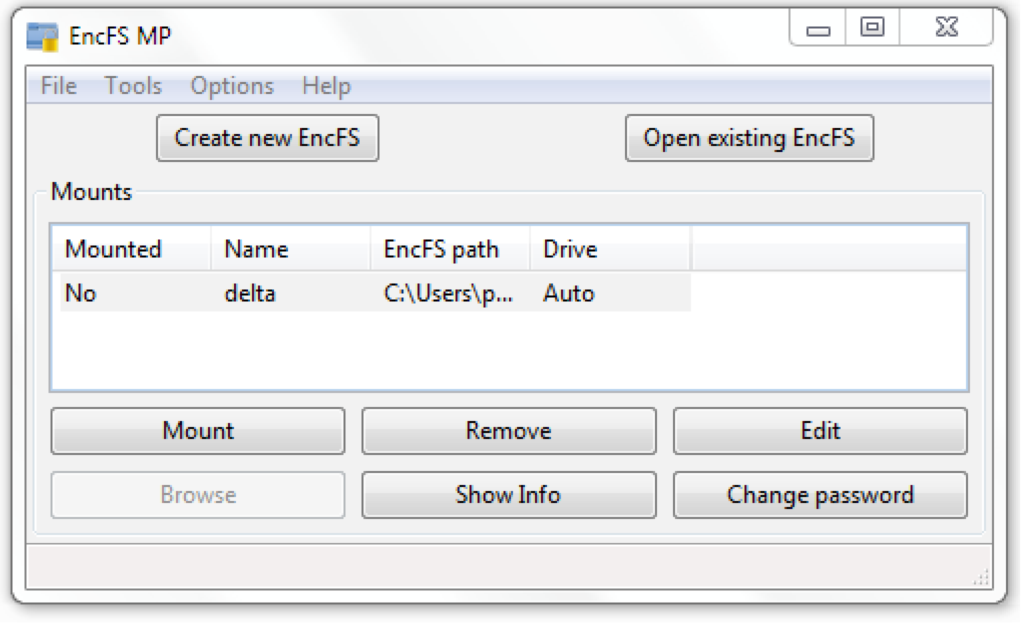
Πριν προχωρήσουμε, οφείλουμε να σταθούμε σε μία ακόμα λεπτομέρεια. Αν ο φάκελος με τα κρυπτογραφημένα αρχεία καταλήγει μέσω του Dropbox και σε άλλους υπολογιστές, είναι βέβαιο ότι θα επιθυμούμε την αποκρυπτογράφησή τους κι εκεί. Η αποκρυπτογράφηση, όμως, προϋποθέτει την παρουσία του αρχείου ρυθμίσεων με το οποίο έγινε η κρυπτογράφηση. Γι' αυτό το λόγο, μια καλή ιδέα θα ήταν να αποθηκεύσουμε το .encfs6.xml μέσα σ' ένα USB stick. Έτσι, το αρχείο ρυθμίσεων θα μας συνοδεύει πάντα και θα μπορούμε να αποκρυπτογραφήσουμε τα αρχεία μας σε οποιονδήποτε υπολογιστή κι αν βρεθούμε.

Χρήση στα Windows

Ας αλλάξουμε τώρα κόσμο κι ας περάσουμε στα Windows. Όπως είπαμε, το EncFS αναπτύχθηκε για το Linux και στηρίζεται στη βιβλιοθήκη FUSE. Επομένως, το ίδιο το EncFS δεν θα μπορούσε να τρέξει στα Windows. Το EncFS όμως αποτελεί προϊόν Ανοιχτού Κώδικα κι αυτό σημαίνει ότι το source code είναι διαθέσιμο σε κάθε ενδιαφερόμενο. Έτσι, με την πάροδο του χρόνου εμφανίστηκαν πολλές εκδοχές του προγράμματος που προσφέρουν την ίδια λειτουργικότητα και είναι προσαρμοσμένες στα

Windows. Αν κάνετε μια σχετική αναζήτηση θα βρείτε αρκετές δημοφιλείς υλοποιήσεις, όπως το encfs4win, το Safe και το EncFSMP. Ξεχωρίσαμε το τελευταίο, καθώς προσφέρει τις περισσότερες επιλογές, αρκετά μεγάλη ταχύτητα και υψηλό επίπεδο συμβατότητας με το "αυθεντικό" EncFS. Το EncFSMP εξάλλου εκτελείται και στο OS X, γεγονός που επεκτείνει το πεδίο εφαρμογής της λύσης που παρουσιάζουμε. Μπορείτε να το κατεβάσετε από τη διεύθυνση http://encfsmp.sourceforge.net.

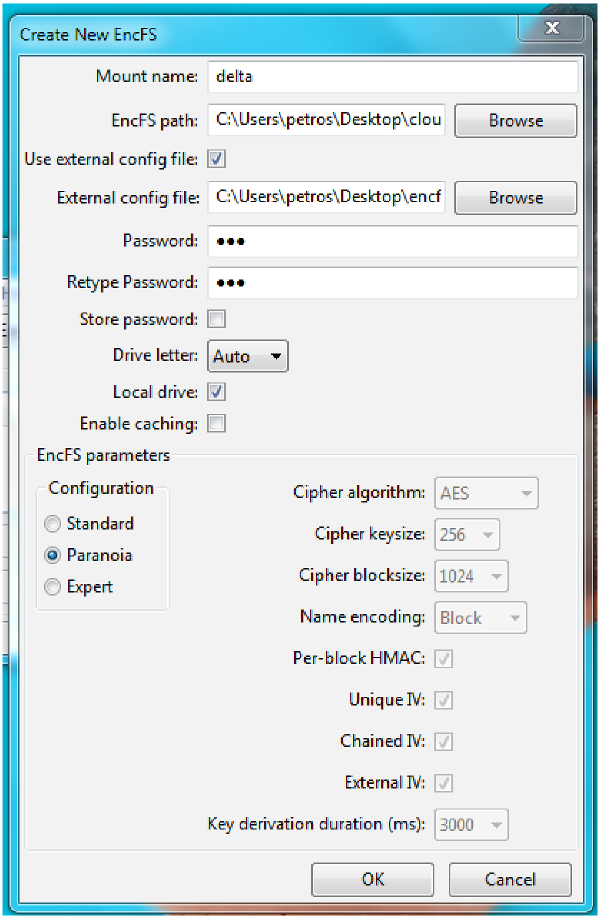
Η εγκατάσταση είναι απλή και δεν απαιτεί κάτι ιδιαίτερο από μέρους μας. Μετά την ολοκλήρωσή της μπορούμε να ξεκινήσουμε το πρόγραμμα από το σχετικό εικονίδιο που θα βρούμε στο μενού "Έναρξη". Από το παράθυρο που εμφανίζεται μπορούμε να επιλέξουμε πρόσθετους φακέλους για την αποθήκευση κρυπτογραφημένων αρχείων, να "συνδεθούμε" σε ήδη υπάρχοντες καταλόγους με κρυπτογραφημένα αρχεία, να αλλάξουμε τις ρυθμίσεις του προγράμματος κ.ο.κ.



Το κεντρικό παράθυρο του EncFSMP παρέχει όλες τις βασικές λειτουργίες του προγράμματος. Από εδώ μπορούμε να προσαρτούμε και να αποπροσαρτούμε καταλόγους με κρυπτογραφημένα αρχεία.

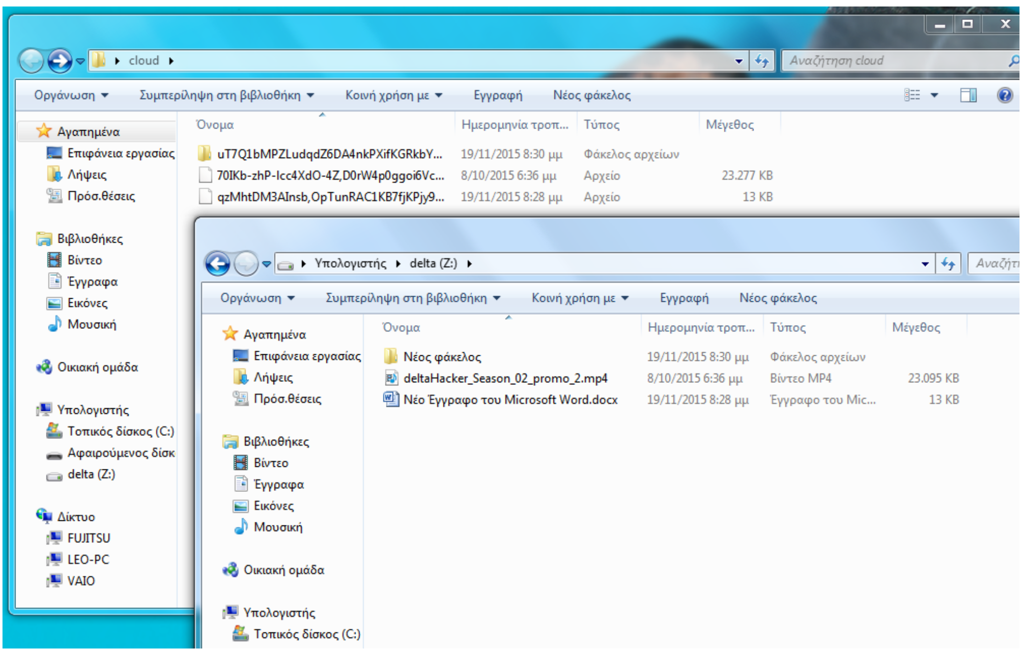
Για τη δημιουργία ενός νέου κρυπτογραφημένου τόμου, αρκεί να πατήσουμε το κουμπί Create new EncFS. Έτσι, εμφανίζεται ένα νέο παράθυρο με όλες τις αναμενόμενες επιλογές. Από εκεί καθορίζουμε τον κατάλογο στον οποίο θα αποθηκεύονται τα κρυπτογραφημένα αρχεία, τον κωδικό κλειδώματος των αρχείων, τις ρυθμίσεις της κρυπτογράφησης και, τέλος, επειδή βρισκόμαστε στα Windows όπου δεν χρησιμοποιούνται κατάλογοι ως mount points, το γράμμα που θα χρησιμοποιείται για την προσάρτηση του εικονικού file system. Όταν ολοκληρώσετε τις ρυθμίσεις και πατήσετε στο κουμπί OK, θα διαπιστώσετε ότι δεν θα συμβεί τίποτα. Αυτό είναι πολύ λο-

γικό, αφού οι ρυθμίσεις μας έχουν αποθηκευτεί κάπου αλλά δεν έχουν εφαρμοστεί πουθενά. Για την εφαρμογή τους πρέπει να προχωρήσουμε στην προσάρτηση του καταλόγου με τα κρυπτογραφημένα αρχεία. Για να γίνει κάτι τέτοιο, από το κεντρικό παράθυρο του προγράμματος επιλέγουμε το όνομα που δώσαμε στον τόμο και πατάμε το κουμπί Mount. Μετά από αυτό, αν ρίξουμε μια ματιά στον Windows Explorer θα διαπιστώσουμε ότι προστέθηκε ένας νέος τοπικός δίσκος. Όπως αντιλαμβάνεστε, μέσα από αυτόν θα έχουμε πρόσβαση στα μη-κρυπτογραφημένα αρχεία, θα μπορούμε να τα τροποποιούμε, να τα διαγράφουμε ή και να προσθέτουμε άλλα. Όπως πάντα, όμως, τα δεδομένα μας θα αποθηκεύονται μόνο σε κρυπτογραφημένη μορφή και μόνο στον κατάλογο που έχουμε επιλέξει. Μια λεπτομέρεια που αξίζει να αναφέρουμε είναι το μέγεθος που φαίνεται να έχει ο δίσκος με τα μη-κρυπτογραφημένα αρχεία. Όπως θα δείτε, το μέγεθός του θα ισούται με τον ελεύθερο χώρο που έχει ο δίσκος εντός του οποίου βρίσκεται ο κατάλογος με τα κρυπτογραφημένα αρχεία. Αυτό συνάδει απόλυτα με τον τρόπο λειτουργίας του προγράμματος, αφού όπως έχουμε πει το EncFS "πατάει" στο υπάρχον σύστημα αρχείων και μπορεί να χρησιμοποιήσει όλο το διαθέσιμο χώρο.



Στην εικόνα βλέπουμε τη δημιουργία ενός νέου εικονικού τόμου. Τα κρυπτογραφημένα αρχεία θα αποθηκεύονται στον κατάλογο C:\users\Petros\Desktop\cloud και η προσάρτησή του θα πραγματοποιείται σε ένα δίσκο με γράμμα που θα επιλέγεται αυτόματα (επιλογή του auto στο πεδίο drive letter). Το όνομα του εν λόγω δίσκου (mount name) θα είναι "delta".

Για την αποπροσάρτηση του ενός τόμου, αρκεί να πατήσουμε το κουμπί Unmount. Όπως θα διαπιστώσατε από τη σύντομη περιγραφή μας, η χρήση του EncFSMP δεν παρουσιάζει καμία δυσκολία. Στις δοκιμές που πραγματοποιήσαμε κατάφερε να αποκρυπτογραφήσει άνετα και χωρίς προβλήματα τα αρχεία που είχαν κρυπτογραφηθεί από το EncFS στο Linux. Φυσικά, η διαφοροποίηση μεταξύ των συστημάτων αρχείων που χρησιμοποιούνται στα δύο λειτουργικά (Ext4 στο Linux και NTFS στα Windows) επιφέρει κάποια μικρά προβλήματα. Το πιο χαρακτηριστικό σχετίζεται με τις ιδιότητες των αρχείων, που σε κάθε λειτουργικό σύστημα είναι εντελώς διαφορετικές. Έτσι, η μόνη ιδιότητα που μοιάζει να λειτουργεί σωστά και στις δύο περιπτώσεις είναι εκείνη της ανάγνωσης – το read only.



Σε πρώτο πλάνο βλέπουμε τη μη-κρυπτογραφημένη εκδοχή των αρχείων, μέσα στον εικονικό δίσκο Z:, που έχει το όνομα "delta". Στο πίσω παράθυρο βλέπουμε την κρυπτογραφημένη εκδοχή των δεδομένων μας, εντός του καταλόγου cloud.

Εν κατακλείδι, πρέπει να τονίσουμε ότι το EncFS δεν προσφέρει ασφάλεια γαλαξιακού επιπέδου. Αυξάνει ωστόσο κατακόρυφα (Σ.τ.Ε. through the roof, βρε παιδί μου) την ασφάλεια που προσφέρει μια υπηρεσία σαν το Dropbox από μόνη της. Εξάλλου, το γεγονός ότι κάθε αρχείο κρυπτογραφείται ξεχωριστά και αποθηκεύεται σε ένα "κανονικό" σύστημα αρχείων, διευκολύνει κατά πολύ τη χρήση υπηρεσιών cloud storage και παρέχει στο EncFS ένα σημαντικό προτέρημα έναντι των υπολοίπων εργαλείων κρυπτογράφησης. Να σημειώσουμε τέλος ότι η ομάδα ανάπτυξης του EncFS είναι ενήμερη για τις θεωρητικές αδυναμίες που έχουν εντοπιστεί και δουλεύει ήδη για την αντιμετώπισή τους. Έχοντας αυτά κατά νου, πιστεύουμε ότι θα αγαπήσετε το EncFS *τουλάχιστον* όσο το αγαπάμε κι εμείς.



e-card
4000 1234 5678 9010
4000
GOOD THRU
MONTH / YEAR 12 / 19
MasterCard
Cardholder Name
Κάρτα e-coin, που δέχεται Bitcoins: Δουλεύει όπως όλες οι κανονικές κάρτες Debit, παντού στον κόσμο και για online αγορές.
Αποκτήστε τη δική σας με κλικ εδώ
και κερδίστε αυτομάτως
25% έκπτωση
κατά την παραγγελία της κάρτας.

Skill: Intermediate
Tags: Wireshark, pfSense, bandwidth hogs, traffic shaping, limiters, aliases, scheduling, firewall rules

Περιορισμός του bandwidth για τους αχόρταγους

Είστε ο υπεύθυνος διαχειριστής ενός δικτύου. Παρατηρείτε ότι κάποιες ώρες μέσα στην ημέρα γίνεται κατάχρηση του bandwidth. Την ίδια στιγμή αρκετοί χρήστες δεν μπορούν να κάνουν τη δουλειά τους. Γίνεστε, φυσικά, ο αποδέκτης των παραπόνων τους. Ποιοι και πώς προκαλούν όλη αυτή την αναστάτωση; Τι μπορείτε να κάνετε ώστε να μην έχετε τέτοιου είδους προβλήματα, από τώρα και στο μέλλον;

του Χρήστου Βαρελά

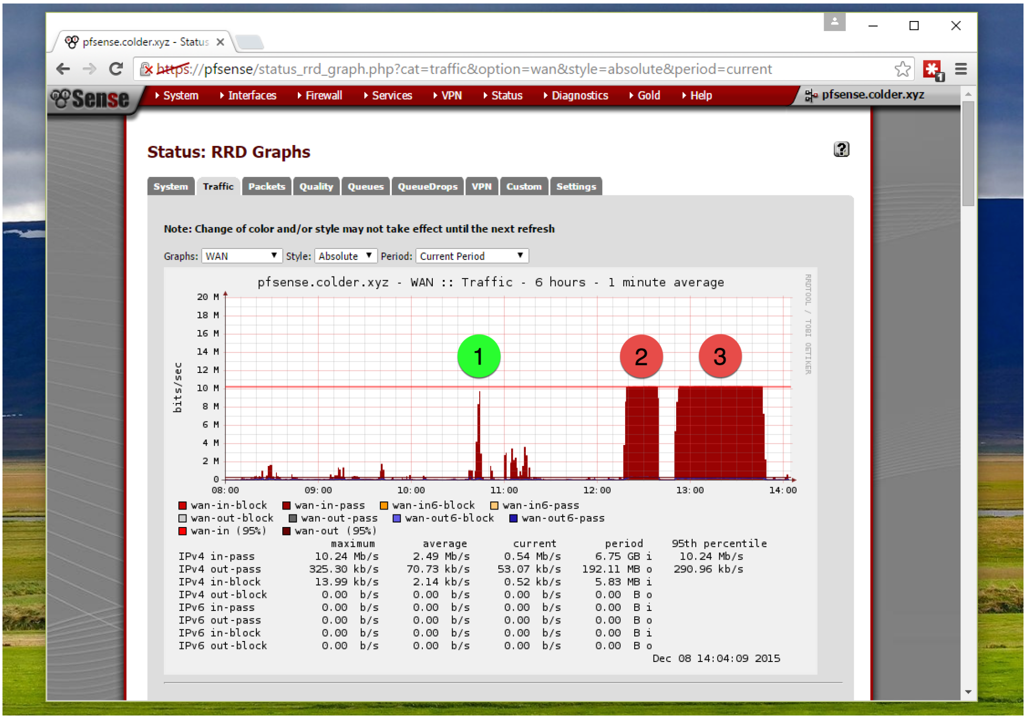
Αναλόγως του bandwidth που διατίθεται για ένα τοπικό δίκτυο, ένας ή δύο χρήστες είναι δυνατόν να το εκμεταλλεύονται σχεδόν αποκλειστικά. Ως αποτέλεσμα, εντελώς ξαφνικά όλοι οι άλλοι χρήστες δυσκολεύονται να κάνουν ακόμη και απλές εργασίες, όπως, π.χ., λήψη email ή web browsing. Η αλήθεια είναι ότι το πρόβλημα με τους λεγόμενους "bandwidth hogs" προκύπτει αρκετά συχνά. Αν μιλάμε για ένα μικρό δίκτυο ο εντοπισμός τους είναι απλός και, προκειμένου να μην έχουμε ξανά παρόμοια προβλήματα στο μέλλον, μερικές συστάσεις ενδεχομένως να αρκούν. Όμως ο καλός διαχειριστής δικτύων δεν σκέφτεται τόσο απλοϊκά – για την ακρίβεια σπάνια έχει αυτή την πολυτέλεια. Πέρα από τις συστάσεις γνωρίζει ότι είναι σημαντικό να επιβάλλει, κεντρικά και με τεχνικά μέσα, συγκεκριμένες πολιτικές συνετής χρήσης.

Στο παρόν άρθρο θα δούμε πώς ανακαλύπτουμε τι προκαλεί την υπερβολική κατανάλωση bandwidth, καθώς και τα μηχανήματα που εμπλέκονται. Γι' αυτή τη δουλειά θα καταφύγουμε στις υπηρεσίες του packet analyzer ονόματι Wireshark. Υποθέτουμε επίσης ότι έχουμε πλήρη πρόσβαση στον router του τοπικού δικτύου, ο οποίος τρέχει το pfSense. Αντί για το pfSense θα μπορούσε να τρέχει το OpenBSD ή κάποια διανομή Linux. Σε κάθε περίπτωση, καταλαβαίνετε ότι δεν μιλάμε για ένα απλό consumer grade router αλλά για κάτι πιο ευέλικτο. Αυτό πάντως που κυρίως μας ενδιαφέρει να παρακολουθήσουμε είναι το σκεπτικό του διαχειριστή δικτύου και, κυρίως, το πώς υλοποιεί μια πολιτική ώστε οι bandwidth hogs να μη δημιουργούν προβλήματα. Έχετε υπόψη ότι τέτοιου είδους πολιτικές δεν βρίσκουν εφαρμογή μόνο σε χώρους εργασίας, αλλά και σε σχολικά/πανεπιστημιακά εργαστήρια ή ακόμη και σε οικιακά δίκτυα, όπου κάποια μέλη έχουν μεγάλο έρωτα με το BitTorrent.

Σημείωση. *Μια καλή εισαγωγή στο Wireshark γίνεται στο δεύτερο άρθρο της μίνι σειράς περί packet analysis (http://deltahacker.gr/?p=8966), στο τεύχος 020 του περιοδικού (http://deltahacker.gr/deltahacker020). Σχετικά με το pfSense, εξάλλου, το αγαπημένο μας λειτουργικό σύστημα για χρήση router/firewall, μπορείτε να παρακολουθήσετε το εκτενές deltaCast s01e07 (http://deltahacker.gr/deltacast-s01e07).*

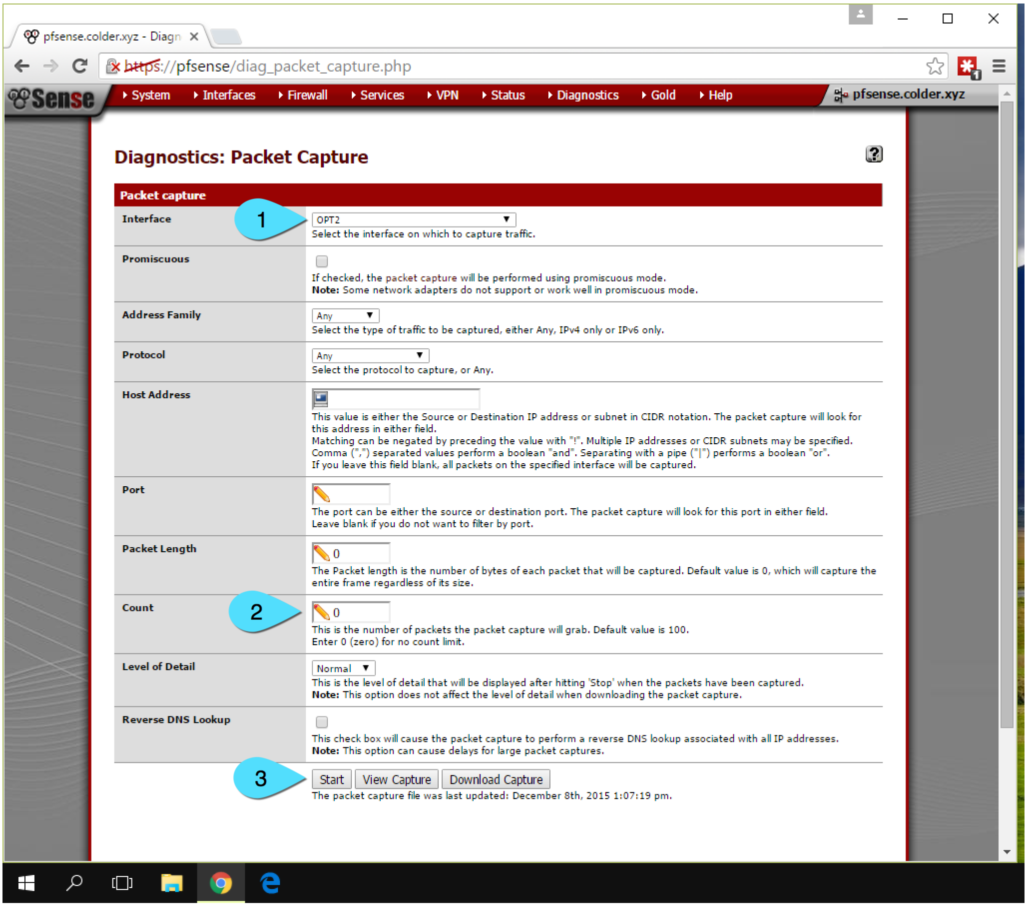
Παρατήρηση του προβλήματος και διερεύνηση

Μέσα από το web panel του pfSense έχουμε πρόσβαση σε μια σειρά από γραφήματα που οπτικοποιούν διάφορες όψεις της συμπεριφοράς του router, καθώς και της κατάστασης που επικρατεί στο τοπικό δίκτυο. Συγκεκριμένα, δίνοντας Status → RDP Graphs κι επιλέγοντας την καρτέλα Traffic, παρακολουθούμε ζωντανά τη δικτυακή κίνηση σε καθένα από τα network interfaces του router. Κάθε φορά που γίνεται κατάχρηση του bandwidth το γεγονός αντικατοπτρίζεται στο γράφημα για το WAN, που είναι το interface με το οποίο το pfSense επικοινωνεί με τον έξω κόσμο. Εκτός από κάποιες –πρακτικά στιγμιαίες– εξάρσεις στη χρήση του bandwidth, τα χρονικά διαστήματα όπου έχουμε κατάχρηση απεικονίζονται ξεκάθαρα. Παρατηρήστε, π.χ., το ακόλουθο screenshot.

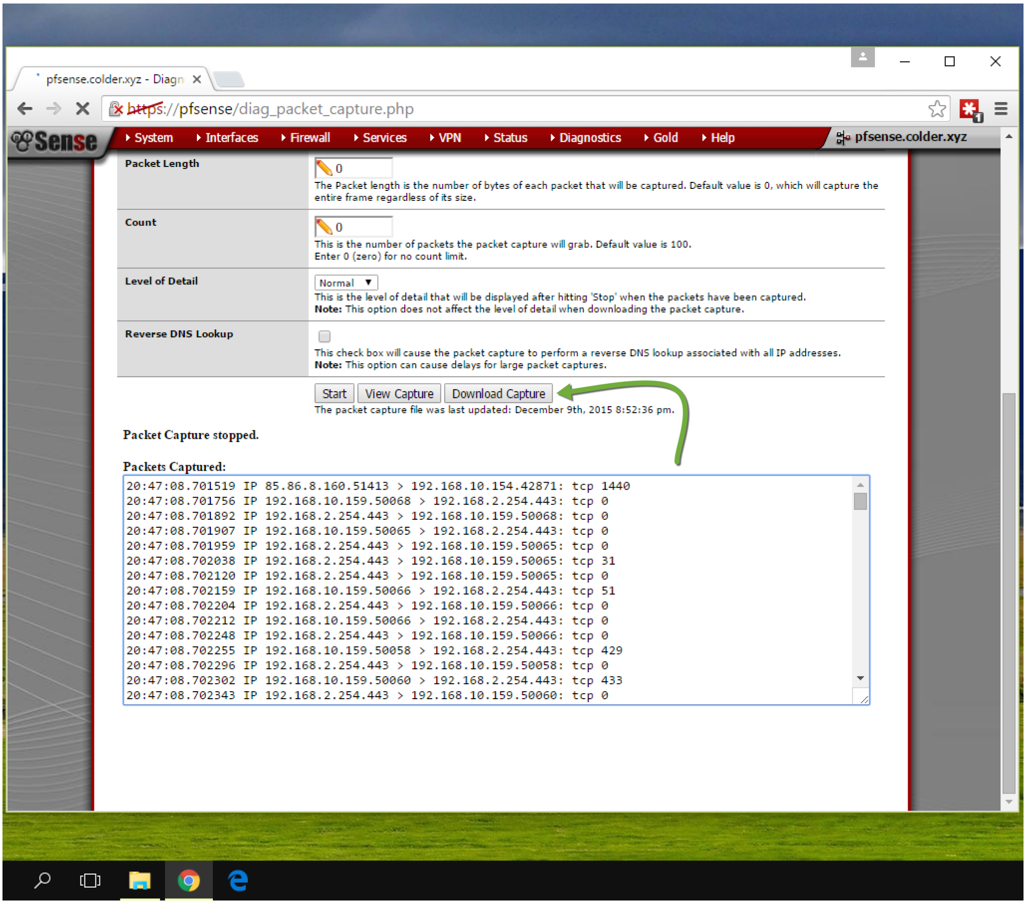


Γραφική αναπαράσταση της δικτυακής κίνησης για το WAN interface του router μας. Υπάρχουν κάποιες περιπτώσεις στιγμιαίας, πρακτικά, έξαρσης στη χρήση bandwidth, οι οποίες δεν δημιουργούν κανένα πρόβλημα απολύτως [βλ. (1)]. Η κατάσταση αλλάζει δραματικά όταν έχουμε παρατεταμένο downloading που αφενός φτάνει στο άνω όριο της γραμμής μας, αφετέρου διαρκεί για αρκετό χρόνο [βλ. (2) και (3)]. Σκεφτείτε ότι όλη αυτή η "κατανάλωση" πιθανώς να οφείλεται σε ένα μόνο μηχάνημα του τοπικού δικτύου, είναι όμως αρκετή ώστε όλοι οι χρήστες να βιώνουν αισθητά περιορισμένη ταχύτητα σύνδεσης, ακόμη και για δραστηριότητες όπως, π.χ., το απλό web browsing.

Θέλοντας να δούμε καλύτερα τι συμβαίνει, δηλαδή ποια μηχανήματα είναι υπεύθυνα για την κατάχρηση και, αν είναι δυνατόν, τι περίπου κάνουν, μια λύση είναι να ξεκινήσουμε μερικά δοκιμαστικά packet captures στο interface που βλέπουν οι πελάτες του pfSense. Το εν λόγω interface για πολλούς θα είναι το LAN, αν κι αυτό δεν είναι απαραίτητο. Στο δικό μας pfSense box, π.χ., το interface που βλέπουν οι clients είναι το OPT2 (bridge των OPT1 και LAN, βλ. http://deltahacker.gr/?p=10507). Προσέξτε: Με packet capture στο WAN ναι μεν θα βλέπουμε με ποια hosts στο Internet επικοινωνεί ο router, αλλά όχι ποια μηχανήματα πίσω του έχουν ξεκινήσει τις αντίστοιχες συνδέσεις. Περιττό να σημειώσουμε ότι τα packet captures καλό είναι να γίνονται όταν παρατηρείται έντονη δικτυακή δραστηριότητα. Τώρα, προκειμένου να ξεκινήσουμε την καταγραφή των πακέτων, από το web panel του pfSense ακολουθούμε τη διαδρομή Disgnostics → Packet Capture.



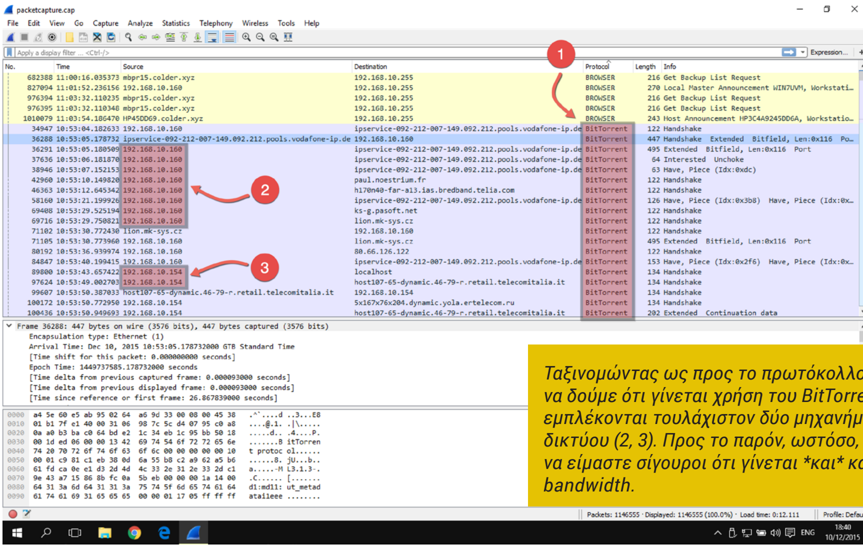
Έτοιμοι για ένα packet capture στο OPT2 (1), το οποίο για την περίπτωσή μας είναι το network interface του router που βλέπουν τα μηχανήματα του τοπικού δικτύου. Αφήνουμε τις προεπιλογές φροντίζοντας μόνο ώστε να ισχύει Count = 0 (2). Έτσι, η καταγραφή των πακέτων θα συνεχίζεται έως ότου αποφασίσουμε να τη διακόψουμε. Η διαδικασία ξεκινά με ένα κλικ στο κουμπί Start (3).



Αφού σταματήσουμε τη διαδικασία της καταγραφής με κλικ στο κουμπί Stop, κάνουμε κι άλλο ένα στο Download Capture. Κατεβάζουμε έτσι το αρχείο ονόματι packetcapture.cap, με όλα τα δικτυακά πακέτα που κατεγράφησαν μόλις. Έχετε υπόψη ότι αν το μέγεθος του αρχείου είναι μεγάλο, ίσως χρειαστεί να περιμένετε λίγο έως ότου ο web browser αρχίσει και πάλι ν' αποκρίνεται. Αν δείτε ότι αργεί να επανέλθει απλά κάντε ένα refresh στη σελίδα και μετά πατήστε ξανά στο Download Capture.

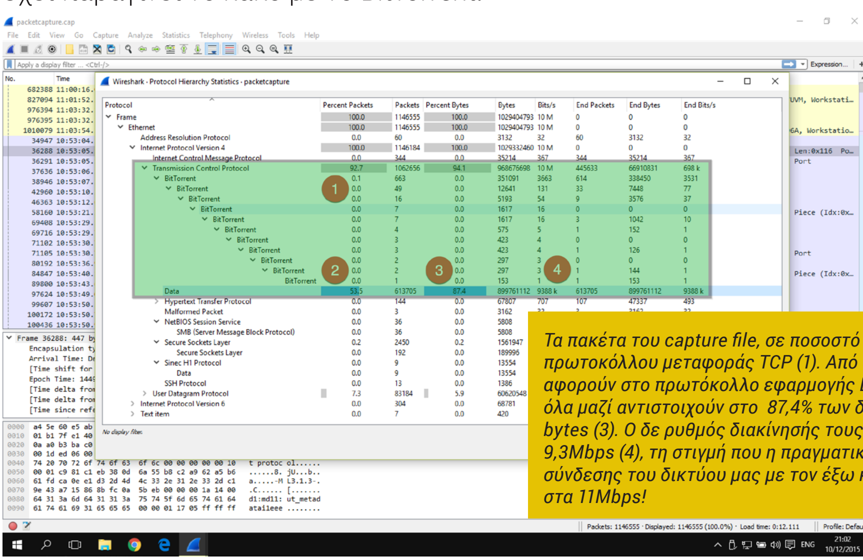
Ανάλυση με το Wireshark

Δουλεύουμε σε περιβάλλον Windows 10 και με την εκδοχή 64bit της πλέον πρόσφατης έκδοσης του Wireshark (2.0.0). Αφού τρέξουμε την εφαρμογή δίνουμε File → Open, μεταβαίνουμε στο φάκελο όπου βρίσκεται το αρχείο packetcapture.cap που πήραμε από το pfSense, το επιλέγουμε και τ' ανοίγουμε. Στο δικό μας παράδειγμα, ταξινομώντας ως προς το πρωτόκολλο (βλ. στήλη Protocol) είναι εύκολο να διαπιστώσουμε ότι γίνεται χρήση του BitTorrent. Αυτό όμως από μόνο του δεν αποτελεί απόδειξη για κατάχρηση.



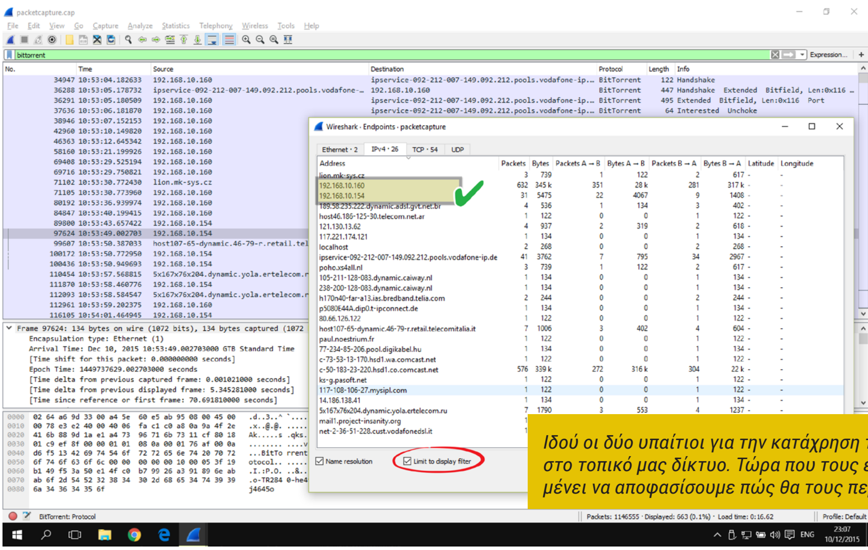
*Ταξινομώντας ως προς το πρωτόκολλο (1) είναι εύκολο να δούμε ότι γίνεται χρήση του BitTorrent, καθώς κι ότι εμπλέκονται τουλάχιστον δύο μηχανήματα του τοπικού δικτύου (2, 3). Προς το παρόν, ωστόσο, δεν μπορούμε να είμαστε σίγουροι ότι γίνεται *και* κατάχρηση του bandwidth.*

Για ν' αποκτήσουμε μια πολύ καλύτερη εικόνα όσον αφορά στα πρωτόκολλα που έπαιζαν στο τοπικό μας δίκτυο κατά τη διάρκεια του capture, από το μενού του Wireshark επιλέγουμε Statistics → Protocol Hierarchy. Αναλόγως του μεγέθους που έχει το capture file ίσως χρειαστεί να περιμένουμε λίγο, τελικά όμως θα εμφανιστεί το παράθυρο ονόματι Protocol Hierarchy Statistics. Σ' αυτό παρατηρούμε ότι τα πακέτα του capture file, σε ποσοστό 92,7% είναι του πρωτοκόλλου μεταφοράς TCP. Από αυτά, το 53,5% αφορούν στο πρωτόκολλο εφαρμογής BitTorrent κι όλα μαζί αντιστοιχούν στο 87,4% των διακινούμενων bytes. Ο δε ρυθμός διακίνησής τους ήταν περί τα 9,3Mbps, τη στιγμή που η πραγματική ταχύτητα σύνδεσης του δικτύου μας με τον έξω κόσμο είναι κοντά στα 11Mbps. Νομίζουμε πως θα συμφωνήσετε κι εσείς ότι έχει παραγίνει το κακό με το BitTorrent.



Τα πακέτα του capture file, σε ποσοστό 92,7% είναι του πρωτοκόλλου μεταφοράς TCP (1). Από αυτά, το 53,5% αφορούν στο πρωτόκολλο εφαρμογής BitTorrent (2) κι όλα μαζί αντιστοιχούν στο 87,4% των διακινούμενων bytes (3). Ο δε ρυθμός διακίνησής τους ήταν περί τα 9,3Mbps (4), τη στιγμή που η πραγματική ταχύτητα σύνδεσης του δικτύου μας με τον έξω κόσμο είναι κοντά στα 11Mbps!

Για να έχουμε στο κεντρικό πλαίσιο του Wireshark μόνο τα BitTorrent packets, στη θυρίδα Expression (στο πάνω μέρος της εφαρμογής) πληκτρολογούμε "bittorrent" (χωρίς τα εισαγωγικά) και πατάμε το [Enter]. Θέλουμε τώρα να βρούμε ποια μηχανήματα του τοπικού δικτύου, που στο παράδειγμά μας έχουν διευθύνσεις IP της μορφής 192.168.10.*, εμπλέκονται σε όλο αυτό το torrenting. Προς τούτο επιλέγουμε Statistics → Endpoints, στο νέο παράθυρο που εμφανίζεται, με όνομα Wireshark - Endpoints - packetcapture, κάνουμε κλικ στην καρτέλα IPv4, μετά τσεκάρουμε και το κουτάκι Limit to display filter. Αμέσως βλέπουμε ότι τα μηχανήματα από τα οποία γίνεται το downloading μέσω BitTorrent είναι τα 192.168.10.154 και 192.168.10.160.



Ιδού οι δύο υπαίτιοι για την κατάχρηση του bandwidth στο τοπικό μας δίκτυο. Τώρα που τους εντοπίσαμε, μένει να αποφασίσουμε πώς θα τους περιορίσουμε.

Στρατηγική αντιμετώπισης

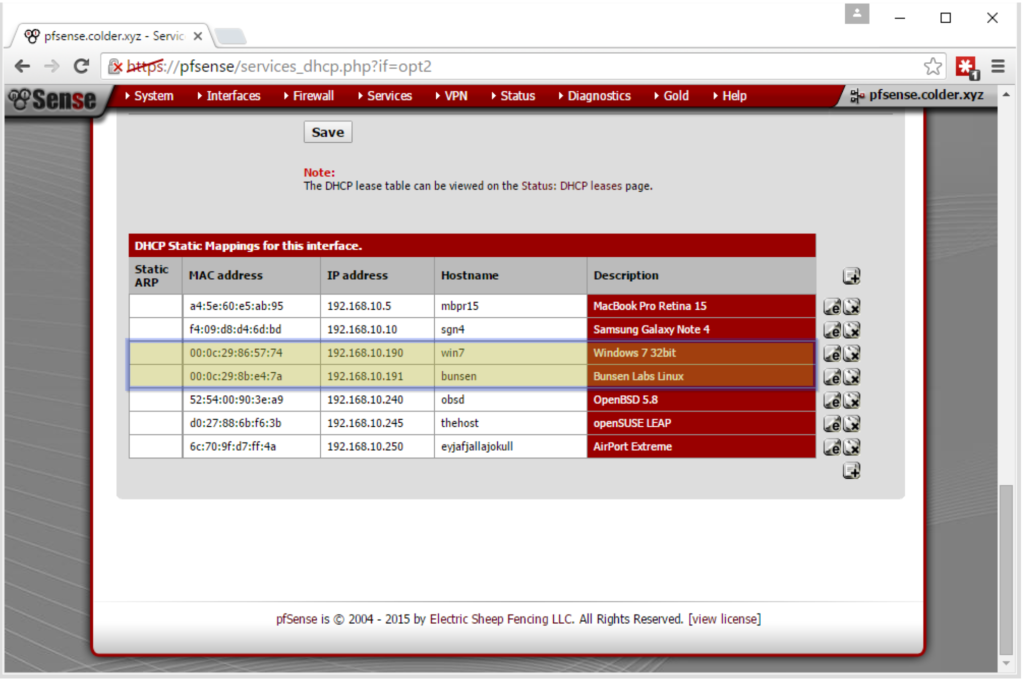
Υπάρχουν πολλά που μπορεί να κάνει ο διαχειριστής ενός δικτύου, προκειμένου να εμποδίσει τους bandwidth hogs από το να προκαλέσουν ξανά προβλήματα στο μέλλον. Μια πρώτη σκέψη είναι να τους απαγορεύεται η πρόσβαση στο Internet, έστω για συγκεκριμένα χρονικά διαστήματα μέσα στο 24ωρο. Θα συμφωνήσετε κι εσείς, φανταζόμαστε, ότι πρόκειται για δρακόντειο μέτρο. Ούτε στο χειρότερο εχθρό μας, ένα πράγμα. Μια ηπιότερη λύση, η οποία φαίνεται να 'χει καλές πιθανότητες να νουθετήσει τους bandwidth hogs επιτρέποντάς τους ταυτόχρονα την πρόσβαση στο Internet, θα ήταν ο περιορισμός του διαθέσιμου bandwidth για εκείνους και μόνο – είτε επί μονίμου βάσεως είτε για συγκεκριμένα διαστήματα μέσα στο 24ωρο.

Είμαστε υπέρ αυτής της δεύτερης προσέγγισης και στο υπόλοιπο του παρόντος εξηγούμε πώς υλοποιείται η σχετική πολιτική. Συγκεκριμένα:

- βάζουμε όλους τους bandwidth hogs στην ίδια λίστα
- ορίζουμε ένα χρονικό διάστημα μέσα στο 24ωρο για τις καθημερινές (όχι για τα σαββατοκύριακα), κατά το οποίο η κατάχρηση του bandwidth πρέπει να αποτρέπεται

- θέτουμε φίλτρα για τον περιορισμό του download, αλλά και του upload rate
- προσθέτουμε έναν νέο κανόνα στο firewall ώστε τα προαναφερθέντα φίλτρα να ισχύουν *μόνο* για τους bandwidth hogs και *μόνο* για το ορισθέν χρονικό διάστημα κατά τις καθημερινές

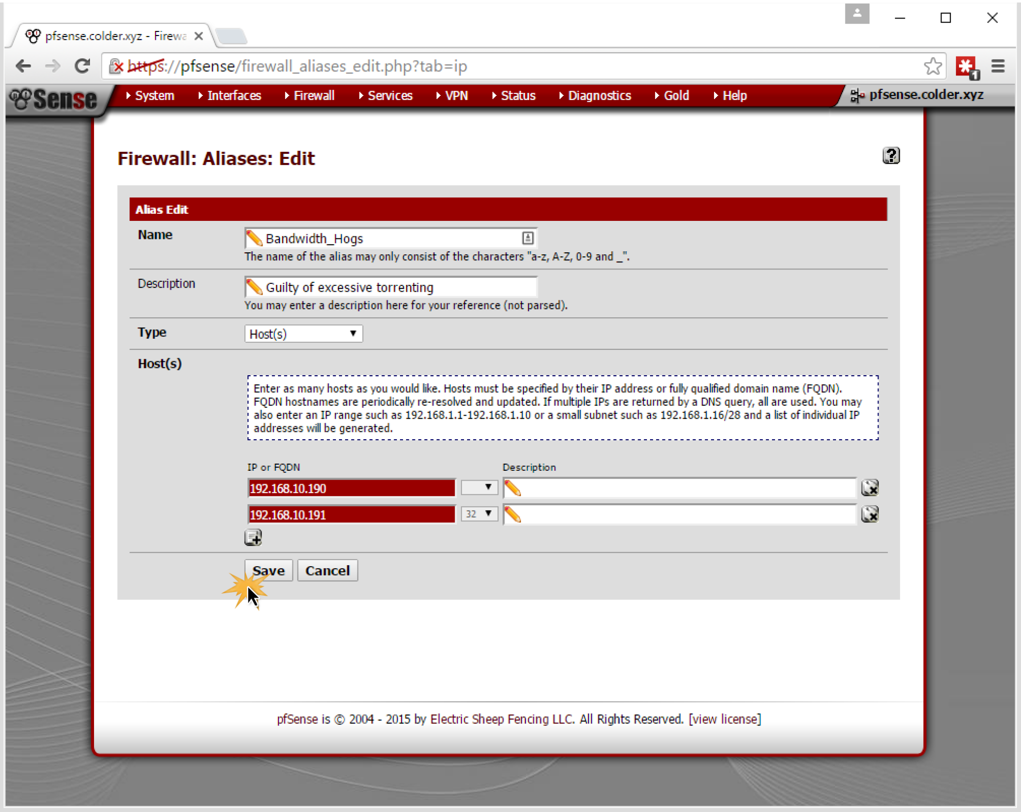
Όλα τα προηγούμενα υλοποιούνται μέσα από το web panel του pfSense και σε πολύ λίγο θα παραθέσουμε όλες τις λεπτομέρειες. Πριν όμως ξεκινήσουμε, να κάνουμε και μια απαραίτητη σημείωση. Στο πλαίσιο του παραδείγματός μας οι bandwidth hogs είναι τα μηχανήματα με διευθύνσεις IP 192.168.10.154 και 192.168.10.160. Αν αυτά δεν έχουν static IP configuration, τότε οι διευθύνσεις IP κάποια στιγμή είναι πολύ πιθανό ν' αλλάξουν κι ως αποτέλεσμα οι περιορισμοί που θα έχουμε θέσει θα πάψουν να ισχύουν ή, ακόμα χειρότερα, θα ισχύουν για τα λάθος μηχανήματα. Ένας τρόπος για ν' αποφύγουμε το πρόβλημα είναι να ρυθμίσουμε τον DHCP server του pfSense, ώστε να δίνει πάντα τις ίδιες διευθύνσεις στους bandwidth hogs. Οι αποδόσεις των διευθύνσεων θα γίνονται βάσει MAC addresses και θα βρίσκονται εκτός του διαστήματος διευθύνσεων που μοιράζει αυτόματα ο DHCP server. Το πώς πετυχαίνουμε κάτι τέτοιο το έχουμε δείξει αρκετές φορές στο παρελθόν (hint: ξεκινήστε από το Status → DHCP Leases). Με βάση τις αναθέσεις διευθύνσεων που εμείς κάναμε, οι δύο bandwidth hogs για τη συνέχεια θα είναι οι 192.168.10.90 και 192.168.10.91.



Φροντίσαμε ώστε στους δύο bandwidth hogs του τοπικού μας δικτύου να αποδίδονται πάντα οι ίδιες διευθύνσεις IP. Έτσι, οι περιορισμοί που σε λίγο θα υλοποιήσουμε θα ισχύουν για τους πραγματικούς υπαίτιους της κατάχρησης bandwidth και μόνον για εκείνους.

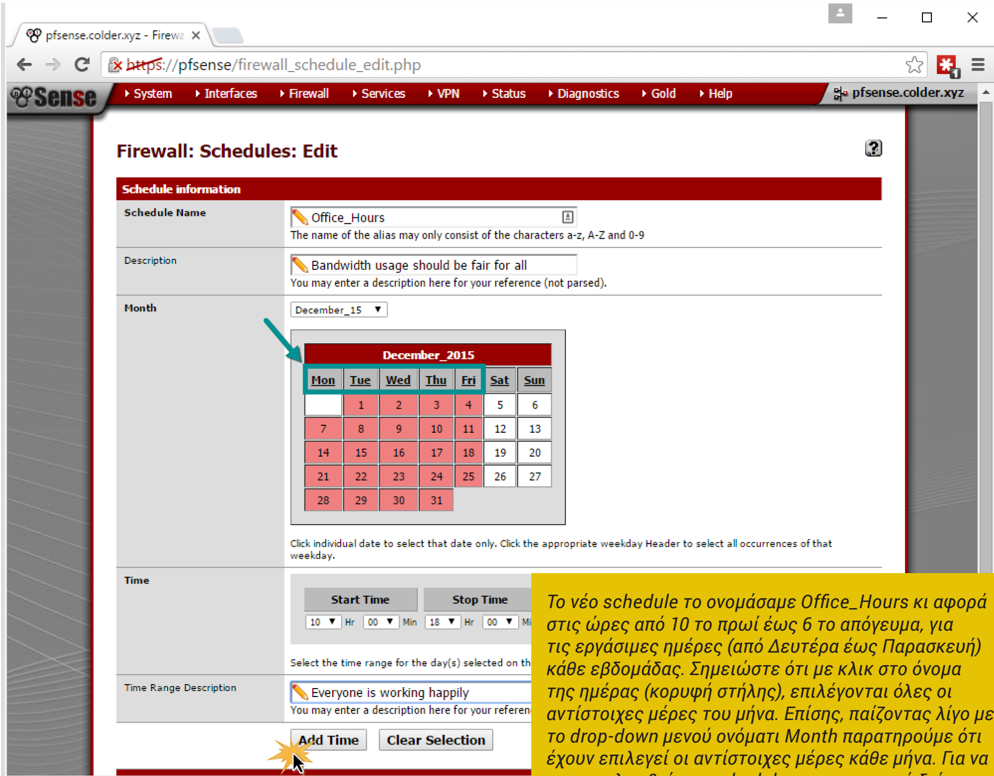
Λίστα με τους bandwidth hogs και ώρες γραφείου

Θέλουμε μία λίστα με τις διευθύνσεις IP των μηχανημάτων από τα οποία γίνεται κατάχρηση του bandwidth. Φυσικά, σ' αυτή τη λίστα θα πρέπει να έχουμε το ελεύθερο για την απομάκρυνση ή/και την προσθήκη διευθύνσεων IP. Αυτό που χρειαζόμαστε είναι ένα νέο alias και για να το ορίσουμε ακολουθούμε τη διαδρομή Firewall → Aliases.

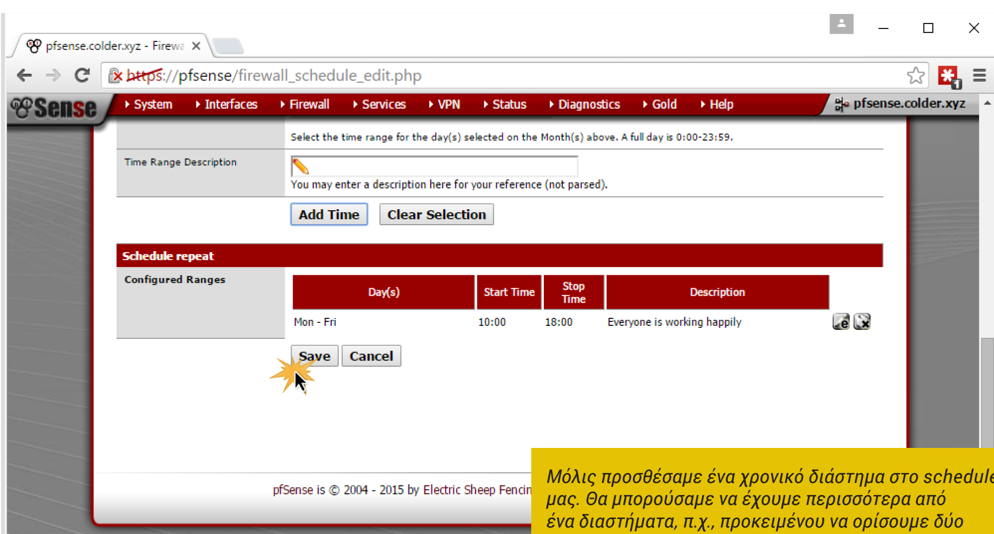


Το alias ονόματι Bandwidth_Hogs, στο οποίο προς το παρόν έχουμε βάλει τα IP των δύο μηχανημάτων από τα οποία αποδεδειγμένα γίνεται κατάχρηση του bandwidth. Εννοείται ότι ανά πάσα στιγμή μπορούμε να προσθαφαιρούμε IPs στην αντίστοιχη λίστα.

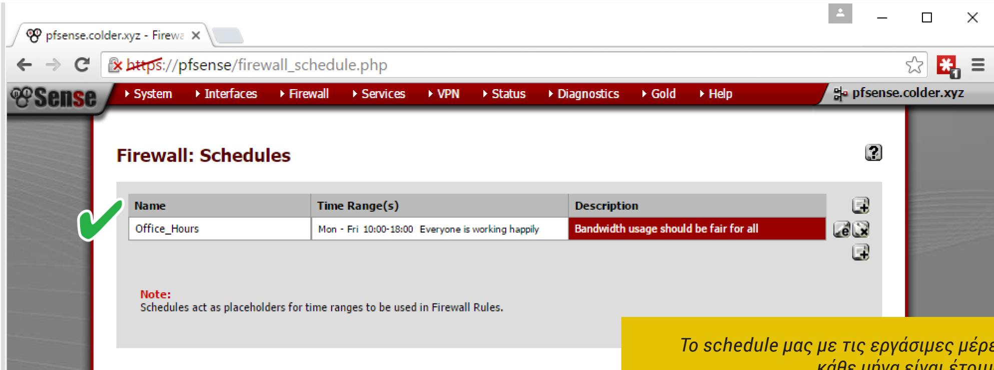
Στη συνέχεια θα ορίσουμε ένα χρονικό διάστημα για τις καθημερινές, κατά το οποίο το bandwidth για όσους είναι στη λίστα Bandwidth_Hogs θα είναι περιορισμένο. Θα δούμε σε λίγο πώς υλοποιείται κάτι τέτοιο. Προς το παρόν, από το μενού του pfSense δίνουμε Firewall → Schedules και κάνουμε ένα κλικ στο κουμπάκι [+], κάτω δεξιά, ώστε να ορίσουμε το νέο "πρόγραμμα" (schedule) που θέλουμε.



Το νέο schedule το ονομάσαμε Office_Hours κι αφορά στις ώρες από 10 το πρωί έως 6 το απόγευμα, για τις εργάσιμες ημέρες (από Δευτέρα έως Παρασκευή) κάθε εβδομάδας. Σημειώστε ότι με κλικ στο όνομα της ημέρας (κορυφή στήλης), επιλέγονται όλες οι αντίστοιχες μέρες του μήνα. Επίσης, παίζοντας λίγο με το drop-down μενού ονόματι Month παρατηρούμε ότι έχουν επιλεγεί οι αντίστοιχες μέρες κάθε μήνα. Για να συμπεριληφθεί στο schedule μας το χρονικό διάστημα που ορίζουμε στην περιοχή Time, αρκεί ένα κλικ στο κουμπάκι Add Time.



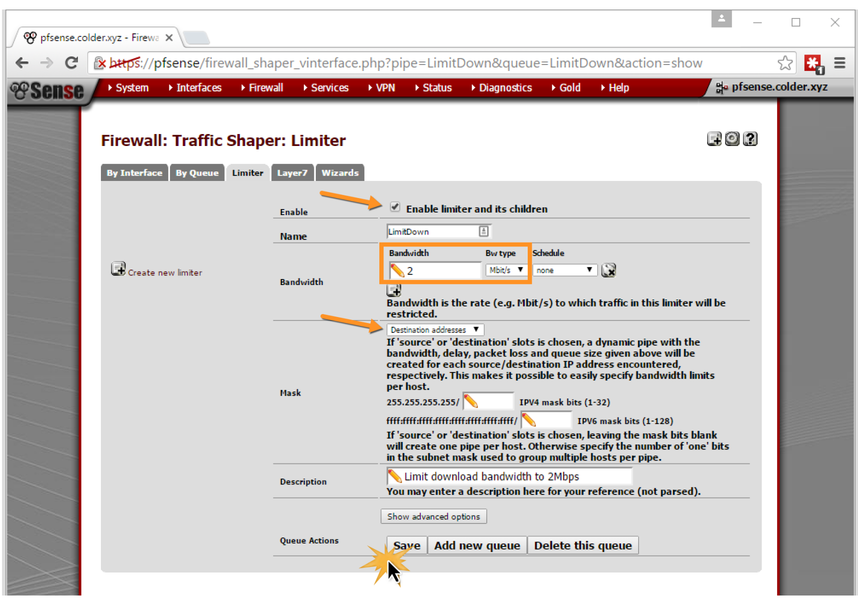
Μόλις προσθέσαμε ένα χρονικό διάστημα στο schedule μας. Θα μπορούσαμε να έχουμε περισσότερα από ένα διαστήματα, π.χ., προκειμένου να ορίσουμε δύο εργάσιμα διαστήματα μέσα στη μέρα, με ένα ημίωρο διάλειμμα ανάμεσά τους.



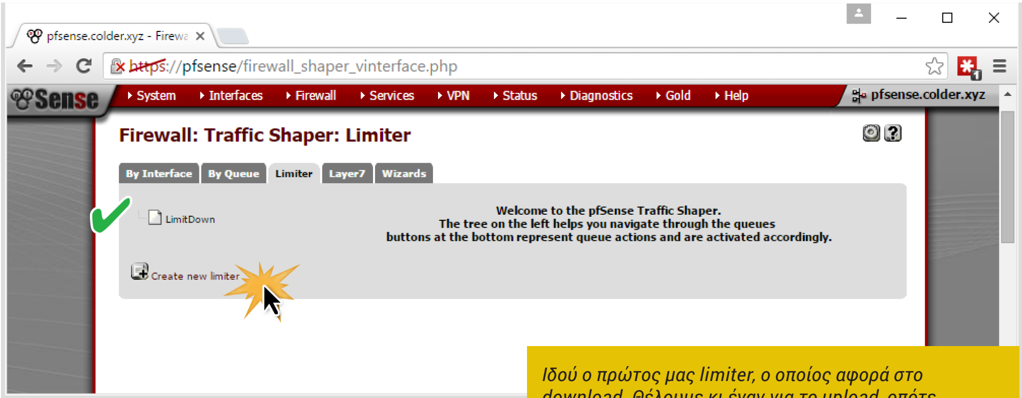
Το schedule μας με τις εργάσιμες μέρες κάθε μήνα είναι έτοιμο.

Limiters για upload και download

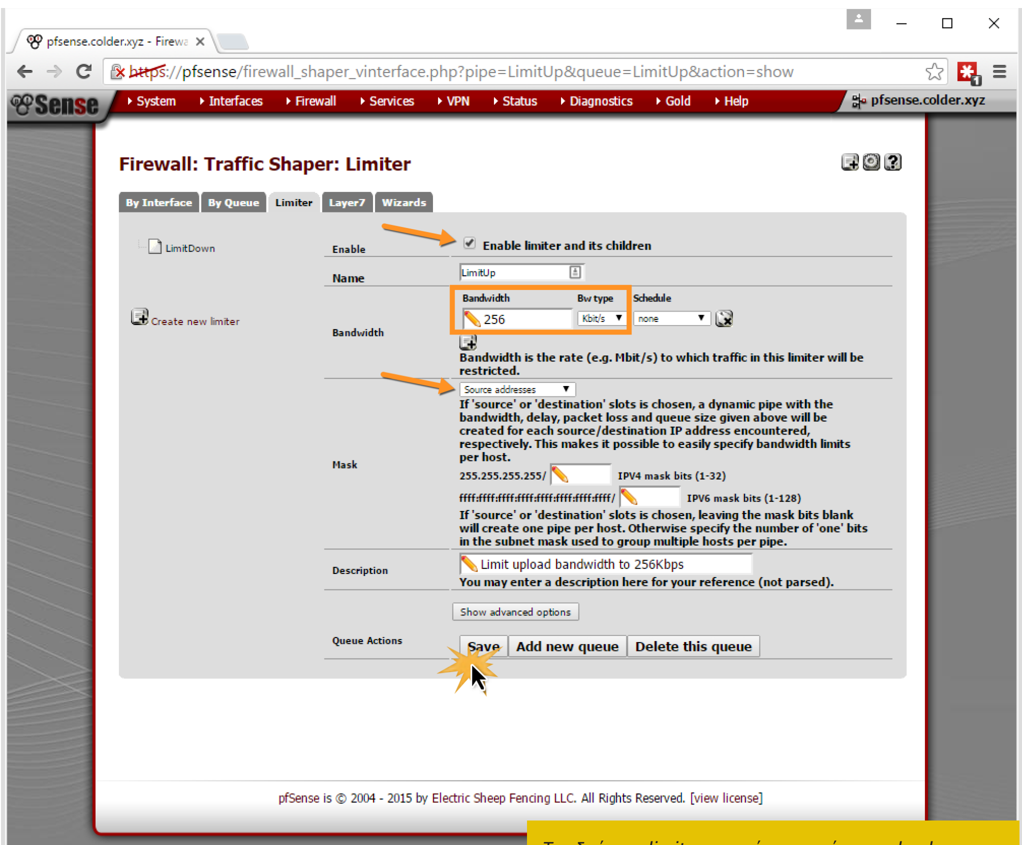
Επόμενη κίνησή μας είναι να ορίσουμε δύο limiters ή φίλτρα, ένα για την ταχύτητα download κι άλλο ένα για την ταχύτητα upload. Αυτά τα φίλτρα θα εφαρμόζονται από κατάλληλο κανόνα του firewall στους υπολογιστές του alias ονόματι Bandwidth_Hosts. Για τον ορισμό ενός limiter ακολουθούμε τη διαδρομή Firewall → Traffic Shaper → Limiter και κάνουμε ένα κλικ στον σύνδεσμο "[+] Create new limiter". Δείτε τα screenshots που ακολουθούν και βεβαίως διαβάστε τις αντίστοιχες περιγραφές.



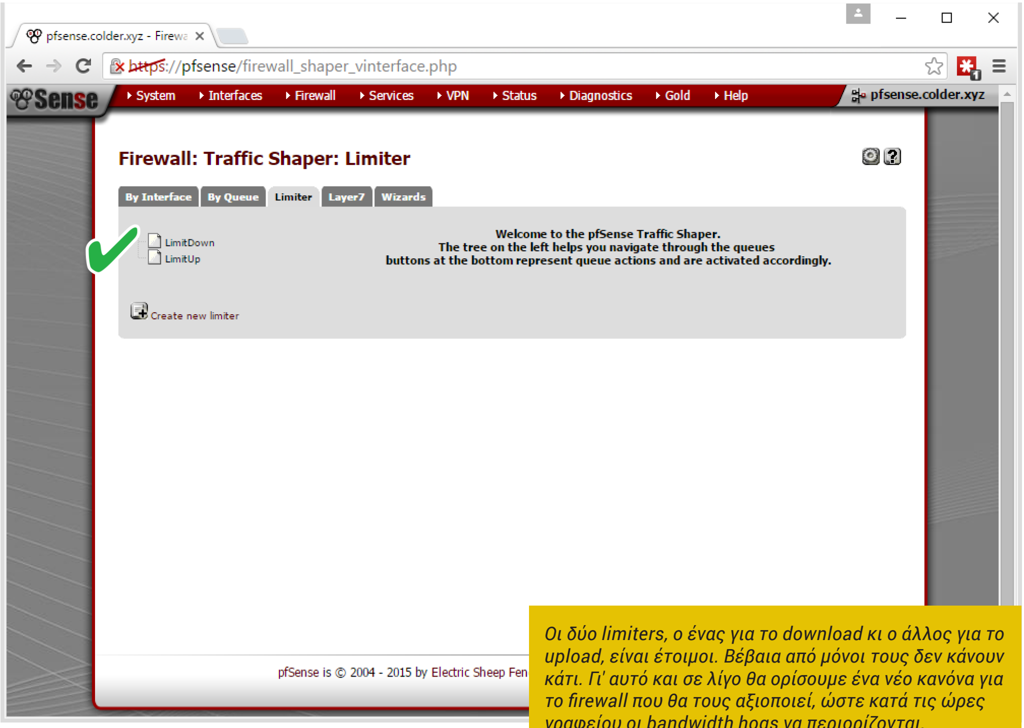
Τον limiter για το download εμείς τον ονομάσαμε LimitDown (θυρίδα Name) κι ως μέγιστη ταχύτητα ορίσαμε τα 2Mbps. Νομίζουμε ότι είναι υπεραρκετή για να παίρνει κάποιος το email του, δεν συμφωνείτε; Στην περιοχή Mask και συγκεκριμένα στο drop-down μενού πάνω πάνω, επιλέξαμε Destination address. Κατ' αυτόν τον τρόπο ο limiter αφορά στο ρυθμό λήψης πακέτων που λαμβάνει κάποιο μηχάνημα του τοπικού μας δικτύου, μ' άλλα λόγια στην ταχύτητα download που μπορεί να έχει. Για να θυμόμαστε αμέσως τι κάνει, γράφουμε αν θέλουμε κάτι περιγραφικό στη θυρίδα Description. Ο limiter δημιουργείται με τσεκάρισμα του Enable limiter and its children, πάνω, βεβαίως και μ' ένα κλικ στο κουμπάκι Save, κάτω.



Ιδού ο πρώτος μας limiter, ο οποίος αφορά στο download. Θέλουμε κι έναν για το upload, οπότε κάνουμε ένα κλικ στο Create new limiter.



Τον δεύτερο limiter, ο οποίος αφορά στο upload, ονομάσαμε LimitUp κι ως μέγιστη ταχύτητα του ορίσαμε τα 256Kbps. Στο drop-down μενού της περιοχής Mask, αυτή τη φορά επιλέξαμε το Source address.



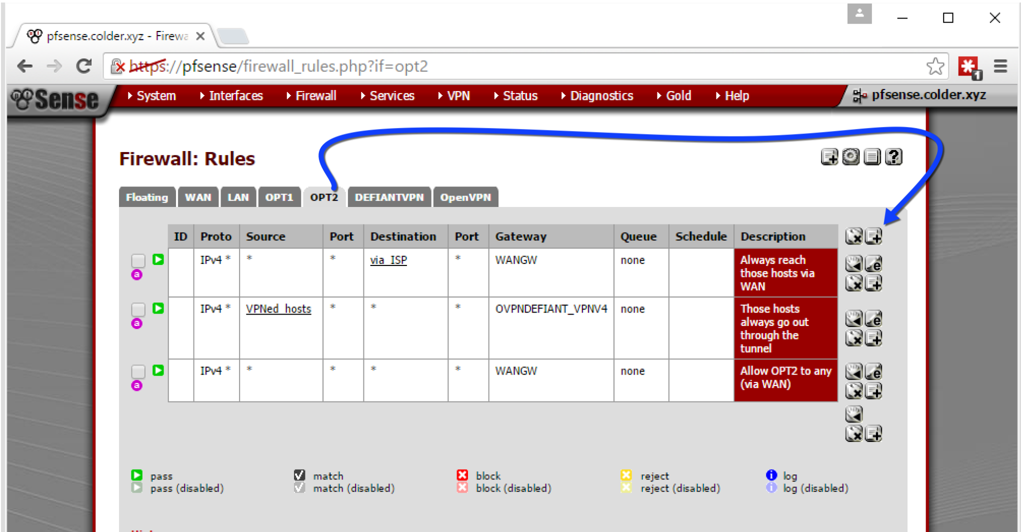
Οι δύο limiters, ο ένας για το download κι ο άλλος για το upload, είναι έτοιμοι. Βέβαια από μόνοι τους δεν κάνουν κάτι. Γι' αυτό και σε λίγο θα ορίσουμε ένα νέο κανόνα για το firewall που θα τους αξιοποιεί, ώστε κατά τις ώρες γραφείου οι bandwidth hogs να περιορίζονται.

Περιοριστικός κανόνας στο firewall

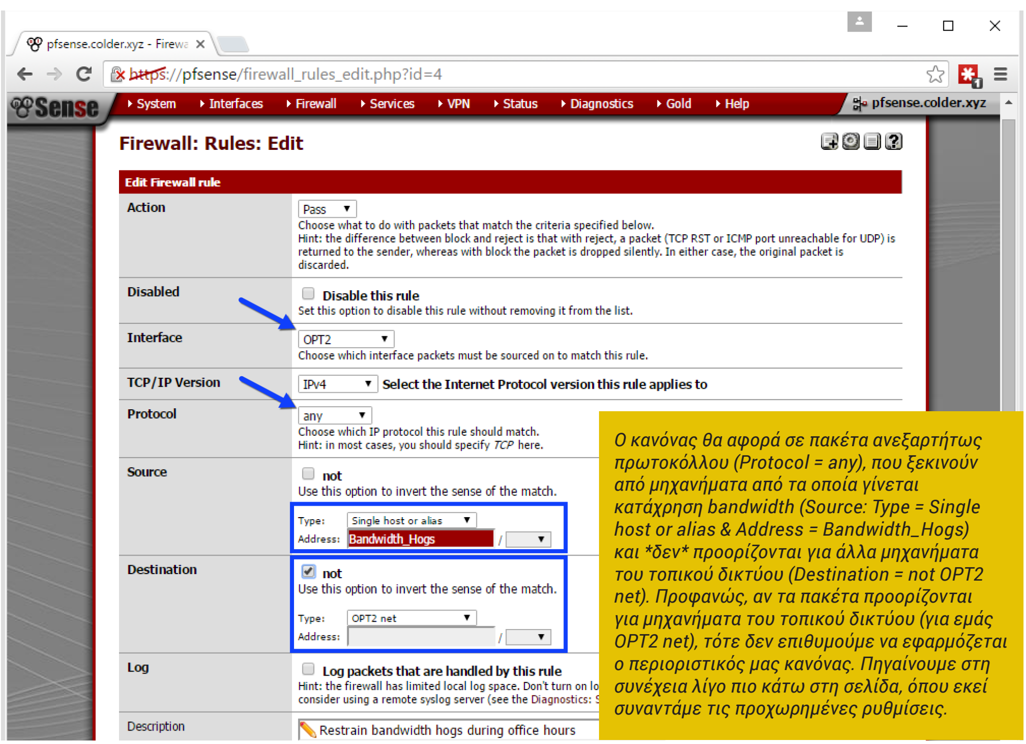
Ως εδώ έχουμε ολοκληρώσει με επιτυχία τις ακόλουθες εργασίες:

- εντοπίσαμε τις διευθύνσεις IP των μηχανημάτων του τοπικού δικτύου, από τα οποία γίνεται κατάχρηση του bandwidth
- φροντίσαμε ώστε τα εν λόγω μηχανήματα (bandwidth hogs) να παίρνουν πάντοτε τις ίδιες διευθύνσεις IP, από τον DHCP server του pfSense
- φτιάξαμε ένα alias με τις διευθύσεις IP των bandwidth hogs
- περιγράψαμε ένα πρόγραμμα (schedule), κατά το οποίο ορίζονται οι εργάσιμες ώρες μέσα στις καθημερινές μέρες κάθε μήνα
- δημιουργήσαμε δύο φίλτρα (limiters), ένα για το download κι ένα για το upload.

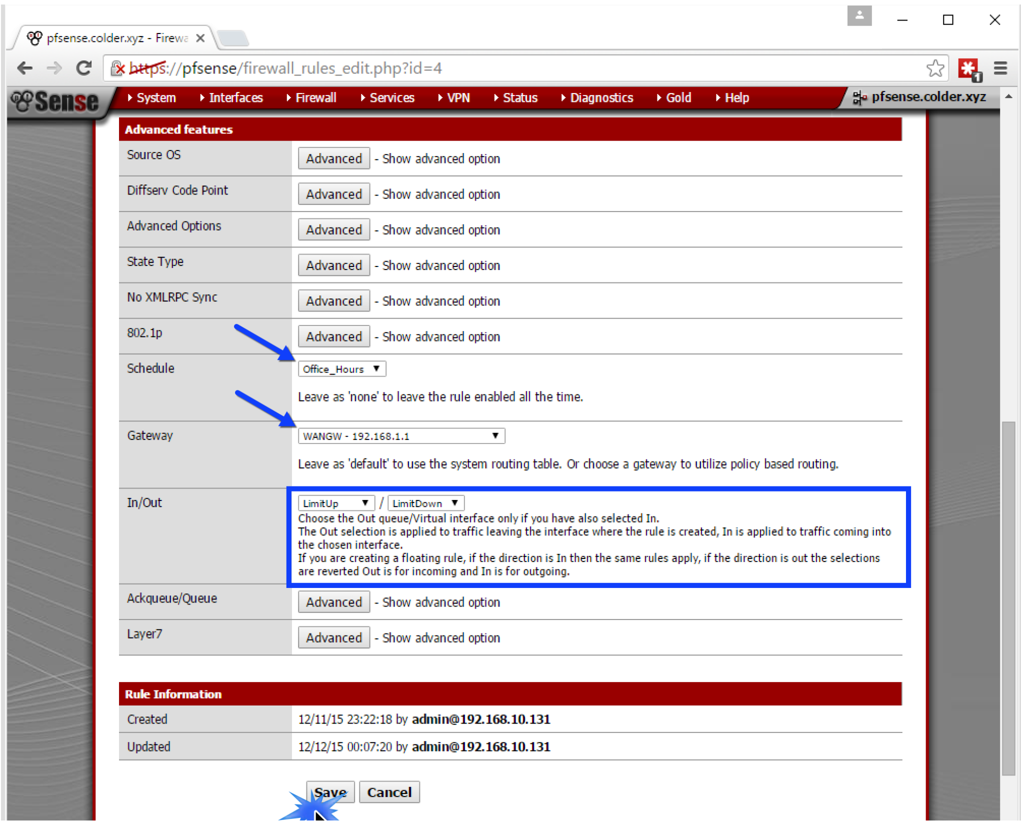
Μένει τώρα να ορίσουμε έναν νέο κανόνα στο firewall του pfSense ο οποίος θα συνδυάζει *όλα* τα προηγούμενα, ώστε οι bandwidth hogs να περιορίζονται κατά τη διάρκεια των εργάσιμων ημερών και ωρών. Δείτε τα screenshots που ακολουθούν.



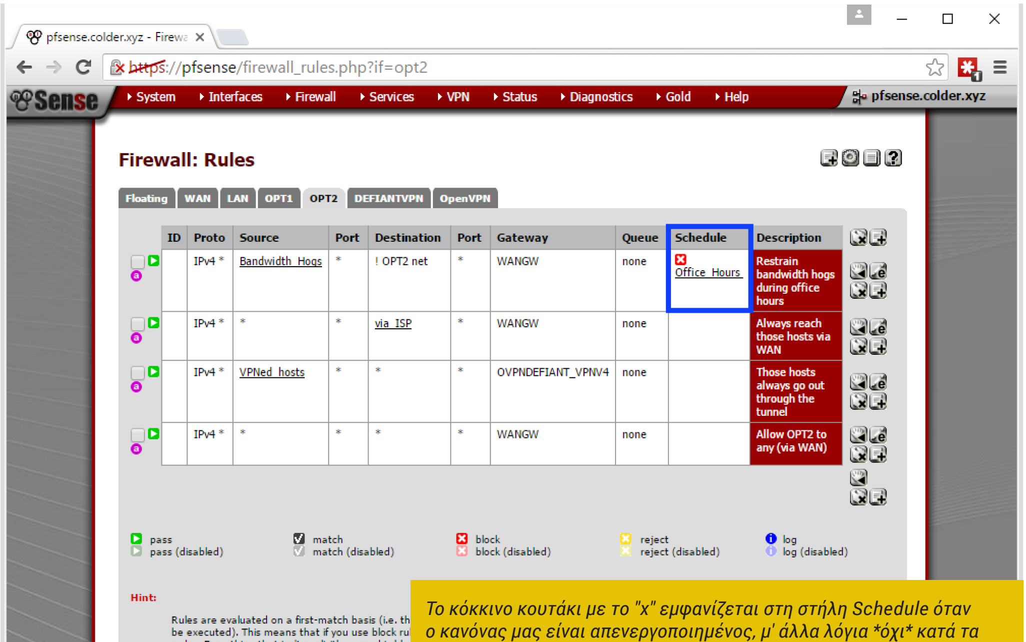
Ξεκινάμε επιλέγοντας Firewall → Rules. Ο κανόνας που θα προσθέσουμε θα αφορά στο network interface που βλέπουν τα μηχανήματα του τοπικού δικτύου. Το interface αυτό εξ ορισμού είναι το LAN — αλλά όχι απαραίτητα. Για το δικό μας δίκτυο, π.χ., το εν λόγω interface είναι το OPT2 (κι αποτελεί bridge των LAN, OPT1). Μεταβαίνουμε, λοιπόν, στην καρτέλα του network interface που μας ενδιαφέρει. Ο περιοριστικός κανόνας που πρόκειται να ορίσουμε επιθυμούμε να ελέγχεται πρώτος, ώστε οι bandwidth hogs να μην έχουν καμία πιθανότητα να "ξεφύγουν". Ακριβώς γι' αυτό κάνουμε ένα κλικ στο κουμπάκι [+], πάνω πάνω δεξιά.



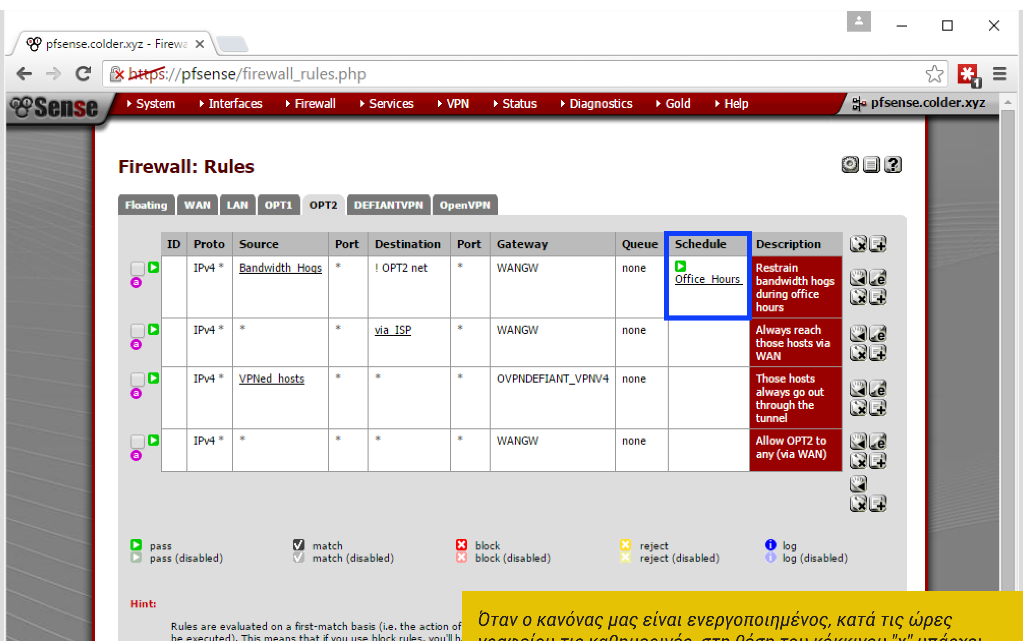
Ο κανόνας θα αφορά σε πακέτα ανεξαρτήτως πρωτοκόλλου (Protocol = any), που ξεκινούν από μηχανήματα από τα οποία γίνεται κατάχρηση bandwidth (Source: Type = Single host or alias & Address = Bandwidth_Hogs) και *δεν* προορίζονται για άλλα μηχανήματα του τοπικού δικτύου (Destination = not OPT2 net). Προφανώς, αν τα πακέτα προορίζονται για μηχανήματα του τοπικού δικτύου (για εμάς OPT2 net), τότε δεν επιθυμούμε να εφαρμόζεται ο περιοριστικός μας κανόνας. Πηγαίνουμε στη συνέχεια λίγο πιο κάτω στη σελίδα, όπου εκεί συναντάμε τις προχωρημένες ρυθμίσεις.



*Ο κανόνας θα είναι ενεργός μόνον κατά τις ώρες γραφείου, όλες τις εργάσιμες μέρες της εβδομάδας. Θέτουμε, λοιπόν, Schedule = Office_Hours. Ο δε gateway μέσω του οποίου τα πακέτα θα βγαίνουν στο Internet δεν χρειάζεται να τεθεί, εκτός αν για τον pfSense router σας υπάρχουν περισσότεροι από ένας gateways. Στον δικό μας, π.χ., πέρα από τον τυπικό έχει οριστεί κι ένας για την επικοινωνία με απομακρυσμένο OpenVPN Access Server που έχουμε στο cloud. Δεν επιθυμούμε οι bandwidth hogs να βγαίνουν στο Internet μέσω του απομακρυσμένου server, οπότε θέτουμε Gateway = WANGW (πρόκειται για το LAN interface του ADSL modem/router μπροστά από το pfSense box). Δώστε τώρα προσοχή στην περιοχή In/Out. Στη θυρίδα του "In" (αριστερά) επιλέγουμε το φίλτρο LimitUp. Έτσι, ο ρυθμός των πακέτων που ξεκινούν από bandwidth hog και *εισέρχονται* στο OPT2 (κατεύθυνση "In") θα περιορίζεται όπως περιγράφει ο limiter ονόματι LimitUp. Διαφορετικά: Το upload rate των bandwidth hogs θα είναι το πολύ 256Kbps. Ομοίως εργαζόμαστε για τη θυρίδα του "Out". Σ' αυτή επιλέγουμε το φίλτρο LimitDown κι έτσι ο ρυθμός των πακέτων που *εξέρχονται* από το OPT2 και προορίζονται προς κάποιον bandwidth hog περιορίζεται όπως περιγράφει ο limiter ονόματι LimitDown. Διαφορετικά: Το download rate των bandwidth hogs θα είναι το πολύ 2Mbps. Για την επικύρωση του κανόνα κάνουμε ένα κλικ στο κουμπί Save.*



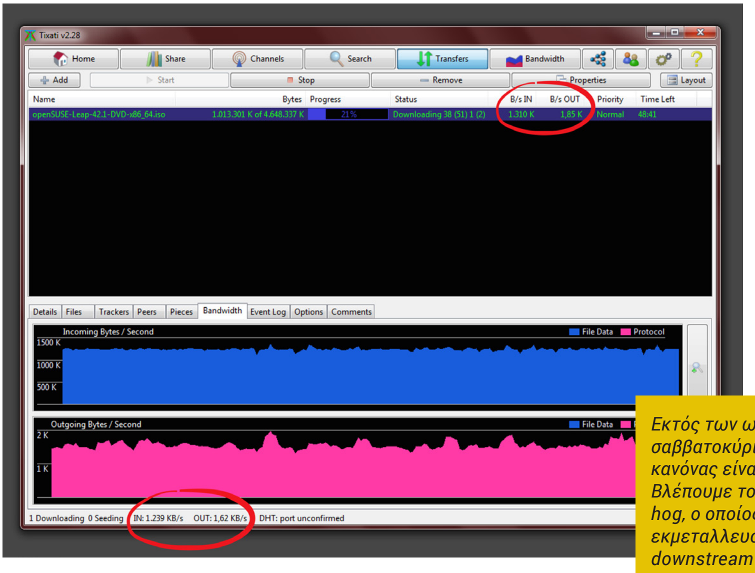
*Το κόκκινο κουτάκι με το "x" εμφανίζεται στη στήλη Schedule όταν ο κανόνας μας είναι απενεργοποιημένος, μ' άλλα λόγια *όχι* κατά τα διαστήματα που ορίζει το πρόγραμμα ονόματι Office_Hours.*



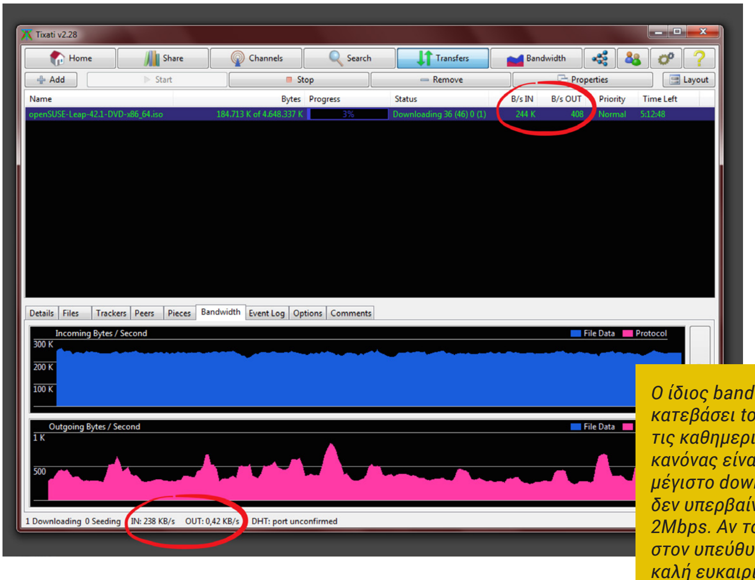
Όταν ο κανόνας μας είναι ενεργοποιημένος, κατά τις ώρες γραφείου τις καθημερινές, στη θέση του κόκκινου "x" υπάρχει ένα πράσινο τετραγωνάκι.

Νέα εμπειρία για τους αχόρταγους

Μετά την εισαγωγή του νέου μας κανόνα η κατάσταση στο τοπικό δίκτυο πίσω από τον pfSense router αλλάζει δραματικά – αλλά μόνο κατά τη διάρκεια των διαστημάτων που ορίζονται από το Office_Hours. Κάντε τις δοκιμές σας, δείτε και δύο στιγμιότυπα των δικών μας.



Εκτός των ωρών γραφείου ή κατά το σαββατοκύριακο, ο περιοριστικός μας κανόνας είναι απενεργοποιημένος. Βλέπουμε το μηχάνημα ενός bandwidth hog, ο οποίος κατεβάζει ένα torrent εκμεταλλευόμενος σχεδόν όλο το downstream bandwidth της σύνδεσής μας προς το Internet.



Ο ίδιος bandwidth hog επιχειρεί να κατεβάσει torrent κατά τις ώρες γραφείου, τις καθημερινές. Ο περιοριστικός μας κανόνας είναι ενεργοποιημένος και το μέγιστο download rate για τον φίλο μας δεν υπερβαίνει τα 256MBps, δηλαδή τα 2Mbps. Αν τολμήσει να παραπονεθεί στον υπεύθυνο δικτύου, θα έχει μια καλή ευκαιρία να ενημερωθεί για τη νέα πολιτική ορθής χρήσης.

Skill: Intermediate
Tags: openSUSE, YaST, KVM, virtualization, VirtIO, pools, direct access

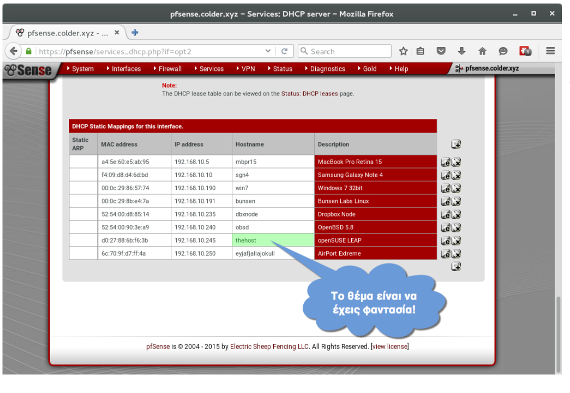
Προσωπικό cloud με το openSUSE

[μέρος 2/2]

Χάρη στο openSUSE μετατρέψαμε ένα μάλλον αδιάφορο PC σε ένα σύγχρονο κι ευέλικτο workstation. Ως τώρα φανταζόμαστε πως κι εσείς θα έχετε εξοικειωθεί κάπως με το ολοκαίνουργιο σύστημά σας. Προτείνουμε λοιπόν να μην καθυστερήσουμε άλλο και να προβούμε τώρα στις απαραίτητες ενέργειες, ώστε να του χαρίσουμε ικανότητες virtualization host. Εκτός από την εγκατάσταση της απαραίτητης υποδομής, θα δούμε βεβαίως και πώς δημιουργούμε και διαχειριζόμαστε εικονικές μηχανές.

του Χρήστου Βαρελά

Πριν περάσουμε στο κυρίως θέμα θα θέλαμε να κάνουμε μια σύντομη σημείωση για τη δικτύωση του PC. Μετά την εγκατάστασή του, το openSUSE είναι έτσι προρυθμισμένο ώστε να ζητά διεύθυνση IP από τον όποιο διαθέσιμο DHCP server. Αν ο name server του τοπικού μας δικτύου είναι στοιχειωδώς ευέλικτος, θα μπορούμε εύκολα να φτάνουμε στο PC γνωρίζοντας μόνο το όνομά του (hostname) κι αγνοώντας εντελώς την αριθμητική διεύθυνση IP. Από τη στιγμή όμως που έχουμε να κάνουμε με μηχάνημα σε ρόλο server, δεν είναι κακή ιδέα να μεριμνήσουμε ώστε να του αποδίδεται πάντοτε το ίδιο IP. Για να πετύχουμε αυτό το αποτέλεσμα δεν χρειάζεται —και δεν προτείνεται— να επέμβουμε στις παραμέτρους δικτύωσης του openSUSE: Αρκεί να επέμβουμε στις ρυθμίσεις του DHCP server που τρέχει ο router *μπροστά* από το PC.

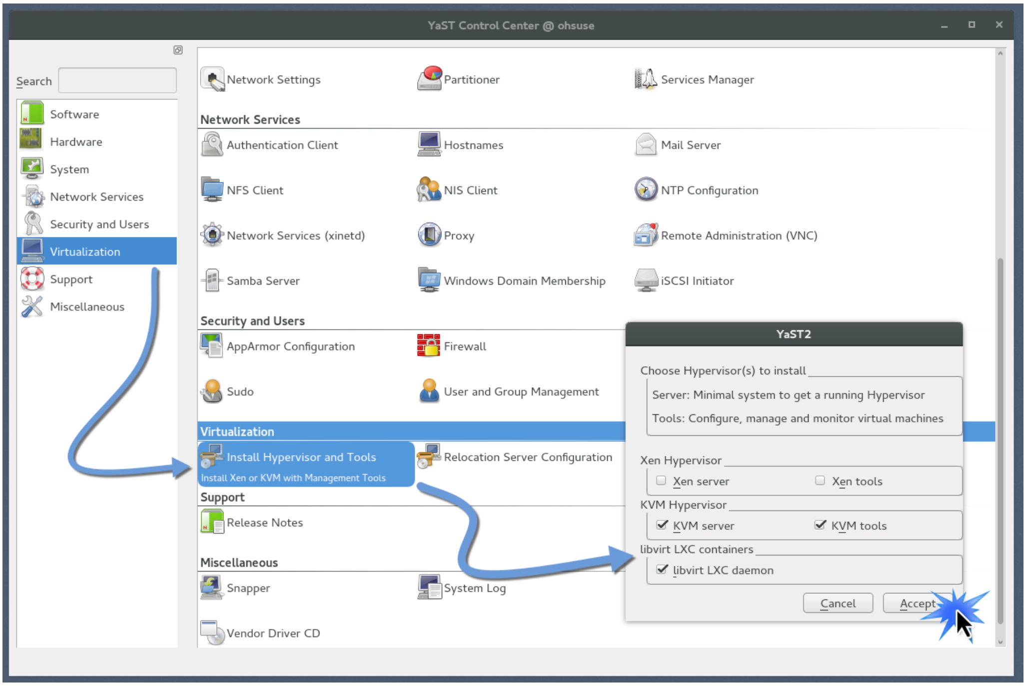


Μετά από αλλεπάλληλες συσκέψεις μεταξύ των συνεργατών του περιοδικού κι ανυπολόγιστη κατανάλωση φαιάς ουσίας, στον ολοκαίνουργιο virtualization host της Parabing Creations αποφασίσαμε να χαρίσουμε το όνομα thehost. Ναι, δεν πρόκειται για τυπογραφικό: thehost. Ακριβέστερα, το πλήρες όνομά του είναι thehost.colder.xyz και, παρεμπιπτόντως, ο DHCP server του router πάντοτε του δίνει την αριθμητική διεύθυνση 192.168.10.245. Και Τώρα Ξέρετε (ΤΜ).

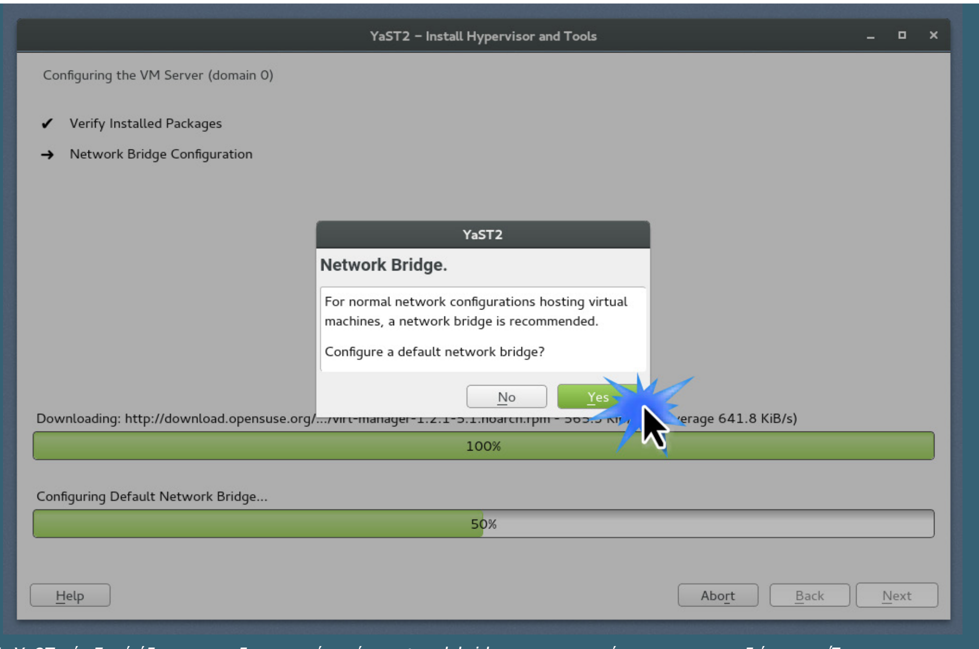
Υποδομή virtualization

Η τεχνολογία virtualization που θα χρησιμοποιεί ο server μας είναι αυτή του KVM (Kernel-based Virtual Machine, http://www.linux-kvm.org). Από την έκδοση 2.60.20 του Linux kernel και μετά, ο κώδικας του KVM περιλαμβάνεται στον πυρήνα. Υπάρχει και το user-space μέρος του KVM, το οποίο συμπεριλαμβάνεται στον πανίσχυρο εξομοιωτή ονόματι QEMU (http://www.qemu.org). Το KVM κάνει δυνατή την εκτέλεση αυτόνομων εικονικών μηχανών, καθεμία από τις οποίες έχει το δικό της εικονικό hardware (δίσκος, κάρτα δικτύου, κάρτα γραφικών κ.ο.κ.) κι ως guest OS τρέχει Linux, Windows ή BSD. Σε σύγκριση εξάλλου με την τεχνολογία virtualization του Xen, το KVM δεν απαιτεί τροποποιημένη εκδοχή του πυρήνα για να λειτουργήσει. Σε μετρήσεις που γίνονται μεταξύ KVM και Xen, οι εικονικές μηχανές του KVM συχνά εμφανίζονται ελαφρώς γρηγορότερες από εκείνες του Xen. Είναι επίσης σημαντικό ν' αναφέρουμε ότι η τεχνολογία του KVM έχει αναδειχθεί στην πλέον δημοφιλή στο cloud. Το VPS σας, μ' άλλα λόγια, είναι πιθανό ν' αποτελεί ένα KVM VM.

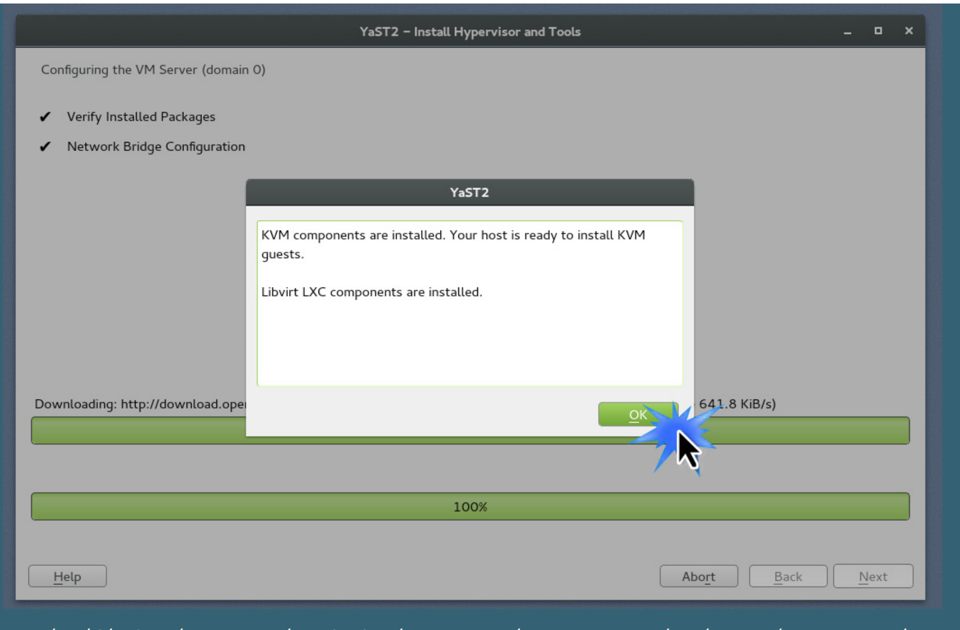
Στο openSUSE μας, ένας τρόπος ώστε να προετοιμαστεί η όλη υποδομή του KVM, μ' άλλα λόγια να εγκατασταθούν τα απαραίτητα εργαλεία και οι βιβλιοθήκες, καθώς και να τροποποιηθεί το υποσύστημα δικτύωσης του host OS, είναι με τη βοήθεια του YaST. Δείτε τα ακόλουθα screenshots και διαβάστε τις αντίστοιχες περιγραφές.



Μέσα από το YaST πηγαίνουμε στην κατηγορία Virtualization κι εκεί επιλέγουμε το Install Hypervizor and Tools. Εμφανίζεται τότε ένα νέο παράθυρο. Στην ενότητα KVM Hypervizor τσεκάρουμε τα KVM server και KVM tools. Προαιρετικά, στην ενότητα libvirt LXC containers τσεκάρουμε και το libvirt LXC daemon. Τα λεγόμενα LXCs (LinuX Containers, https://en.wikipedia.org/wiki/LXC) συγγενεύουν με τα FreeBSD jails, αποτελούν μια μορφή "ελαφριού" virtualization κι επιτρέπουν την εκτέλεση αυτόνομων συστημάτων Linux κάτω από τον ίδιο Linux host. Για να ξεκινήσει η εγκατάσταση της υποδομής virtualization αρκεί ένα κλικ στο κουμπί Accept.



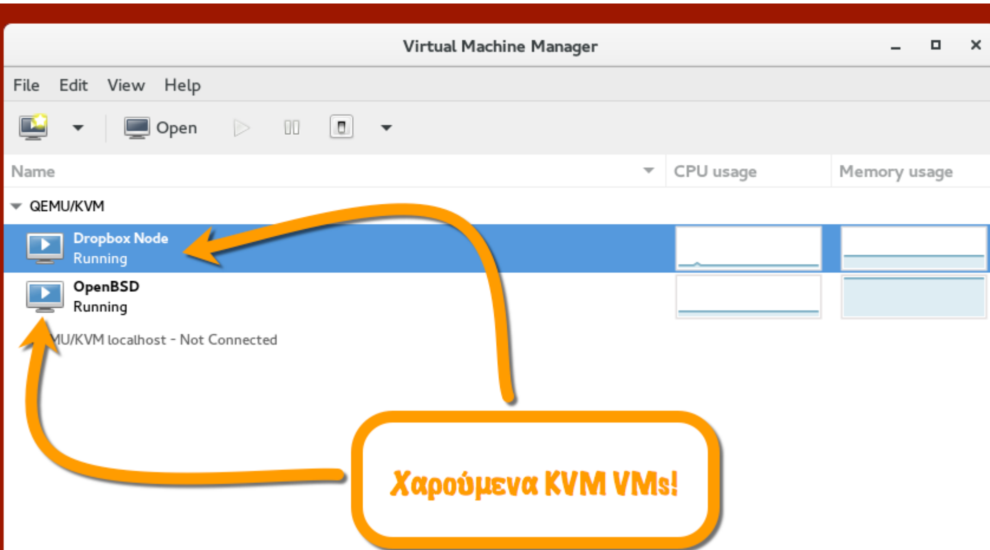
Το YaST μάς ζητά άδεια για να δημιουργήσει ένα network bridge – και προτείνεται να του τη δώσουμε. Έτσι, οι εικονικές μας μηχανές θα είναι σε θέση να λαμβάνουν διευθύνσεις IP απευθείας από τον router του τοπικού δικτύου στον οποίο κατοικεί ο host.



Μετά από λίγα λεπτά το YaST θα έχει ολοκληρώσει τις εργασίες του και το μηχάνημά μας θα έχει μετατραπεί σε έναν ικανότατο virtualization host.

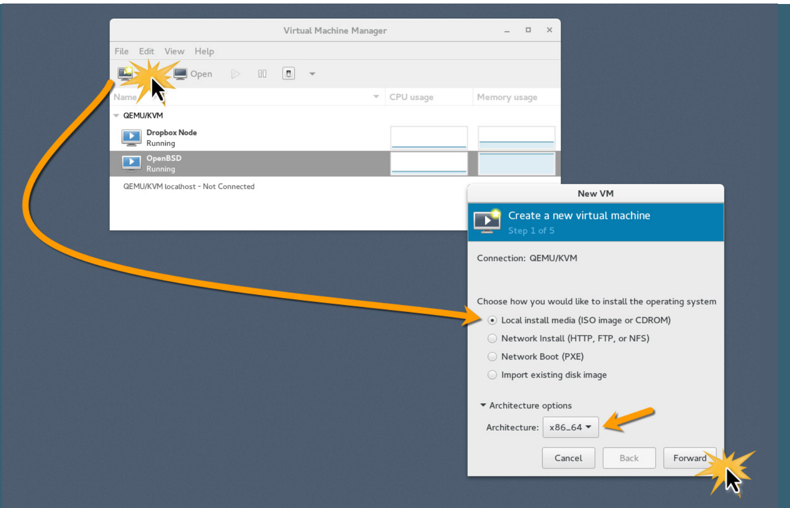
Γνωριμία με τον Virtual Machine Manager

Η δημιουργία και η διαχείριση εικονικών μηχανών είναι δυνατόν να γίνονται από τη γραμμή εντολών. Για όσους όμως τώρα ξεκινούν με το KVM, μια εφαρμογή για το περιβάλλον γραφικών όπως ο Virtual Machine Manager είναι σίγουρα προτιμότερη. Η εν λόγω εφαρμογή εγκαταστάθηκε πριν λίγο, από το YaST. Το όνομα του εκτελέσιμου είναι virt-manager και το πληκτρολογούμε είτε στη γραμμή εντολών είτε στη θυρίδα αναζήτησης του GNOME desktop. Σε κάθε περίπτωση θα μας ζητηθεί να πληκτρολογήσουμε το password του χρήστη μας. Φυσικά, το εικονίδιο του Virtual Machine Manager μπορούμε να το έχουμε στην αριστερή κάθετη μπάρα του GNOME.

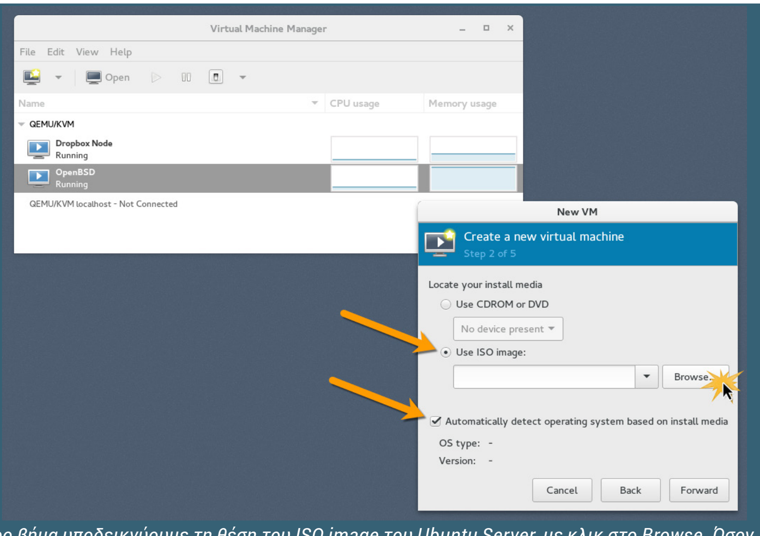


Το κεντρικό παράθυρο του Virtual Machine Manager της εγκατάστασής μας, στο οποίο φαίνονται δύο ενεργές εικονικές μηχανές.

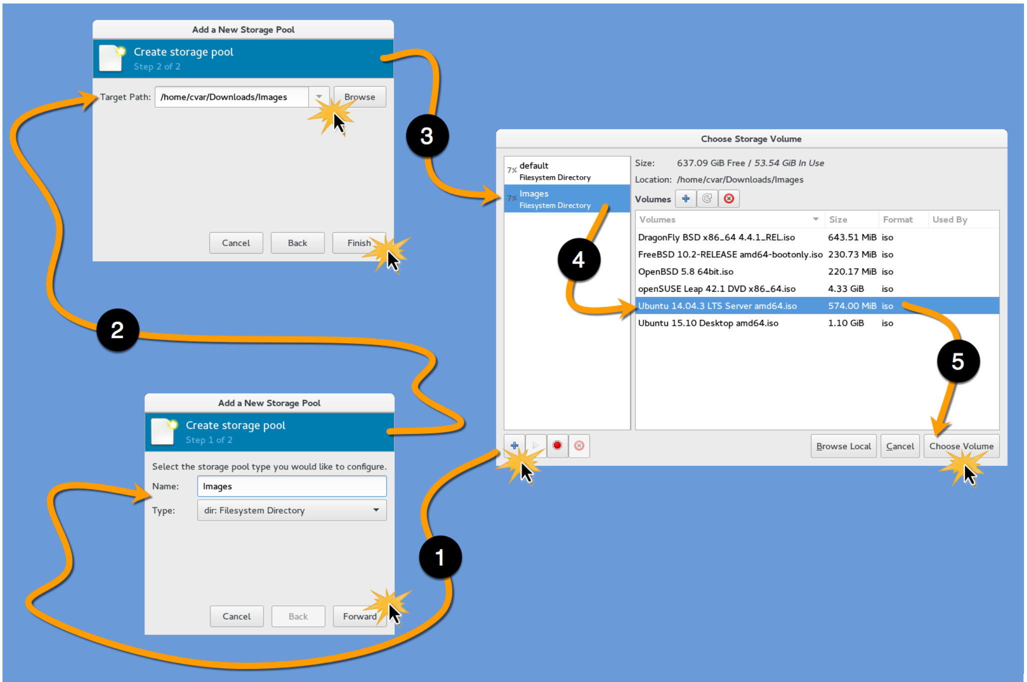
Παρατηρώντας για πρώτη φορά τον Virtual Machine Manager πιθανώς να μας φανεί φτωχικός και μάλλον δεν θα μας κερδίσει. Ωστόσο η εφαρμογή παρέχει μεγάλη ευκολία αλλά *και* ευελιξία. Ο καλύτερος τρόπος για να το διαπιστώσουμε είναι δημιουργώντας μια εικονική μηχανή. Στο πλαίσιο του παραδείγματος που ακολουθεί, το VM που φτιάχνουμε για λειτουργικό σύστημα (guest OS) έχει το Ubuntu Server 14.04.3 LTS 64bit. Πριν ξεκινήσουμε οφείλουμε φυσικά να έχουμε κατεβάσει το αντίστοιχο ISO image, εν προκειμένω εκείνο από το http://www.ubuntu.com/download/server. Δείτε τα screenshots και διαβάστε τις αντίστοιχες περιγραφές.



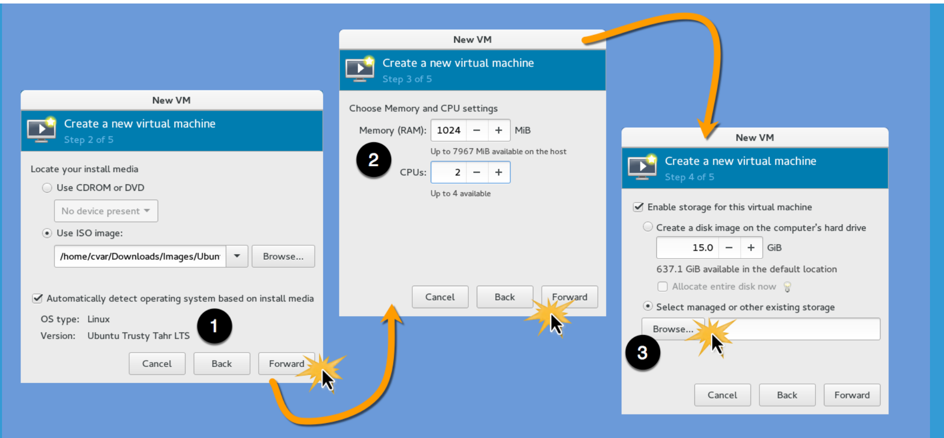
Η δημιουργία μιας νέας εικονικής μηχανής ξεκινά με κλικ στο σχετικό εικονίδιο, πάνω αριστερά και κάτω από το μενού του Virtual Machine Manager. Ανοίγει τότε ένα νέο παράθυρο, το οποίο ουσιαστικά αποτελεί έναν βήμα-προς-βήμα οδηγό. Όπως βλέπετε κι εσείς, όλα τα βήματα είναι μόλις πέντε. Καλό αυτό. Στο πρώτο βήμα οφείλουμε να υποδείξουμε το ISO image του λειτουργικού συστήματος που θα έχει η μηχανή. Το έχουμε ήδη κατεβάσει στον host, οπότε επιλέγουμε το Local install media (ISO image or CDROM). Το λειτουργικό μας θα είναι 64bit, επομένως η μηχανή πρέπει να έχει την ανάλογη αρχιτεκτονική. Θέτουμε, λοιπόν, Architecture = x86_64 κι ακολούθως κάνουμε ένα κλικ στο κουμπάκι Forward, κάτω δεξιά.



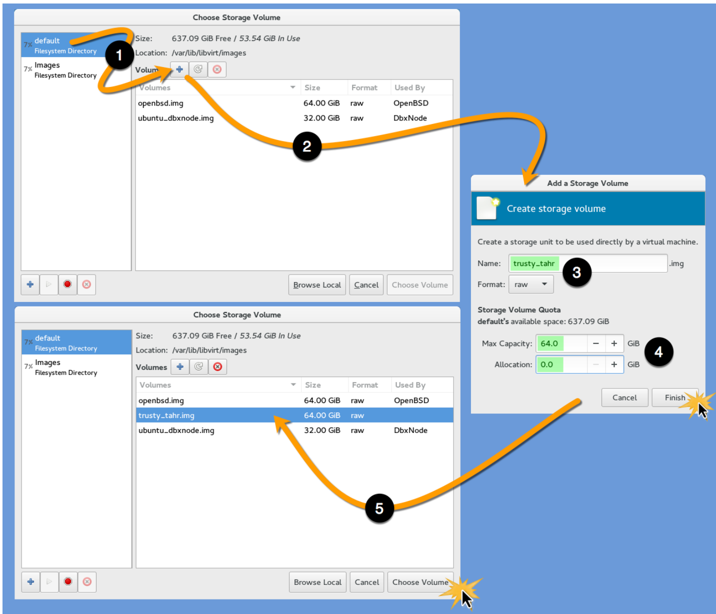
Στο δεύτερο βήμα υποδεικνύουμε τη θέση του ISO image του Ubuntu Server, με κλικ στο Browse. Όσον αφορά στον τύπο του λειτουργικού συστήματος που θα έχει το νέο VM, παρατηρήστε ότι έχουμε τσεκάρει το Automatically detect operating system based on install media. Με τη συγκεκριμένη επιλογή λέμε στον Virtual Machine Manager να προσπαθήσει και να βρει τον τύπο του λειτουργικού αυτόματα, βασιζόμενος στα περιεχόμενα του μέσου εγκατάστασης. Αν δεν τα καταφέρει ή τέλος πάντων διαπιστώσουμε ότι δεν έκανε και πολύ καλή δουλειά, αποεπιλέγουμε το Automatically detect... κι από τα OS type και Version καθορίζουμε μόνοι μας το λειτουργικό. Είναι πιθανό να διαπιστώσουμε ότι δεν παρέχεται ακριβής επιλογή για τον τύπο ή για την έκδοση του λειτουργικού που θα έχει το VM μας. Σε μια τέτοια περίπτωση δεν πρέπει να πτοηθούμε κι αρκεί να καθορίσουμε τον πιο κοντινό τύπο ή την πιο κοντινή έκδοση. Παράδειγμα: Για ένα KVM VM με guest OS το OpenBSD 5.8 64bit, εμείς θέσαμε OS Type = UNIX και Version = OpenBSD 5.6. Όλα πήγαν καλά, περιττό να σημειώσουμε.



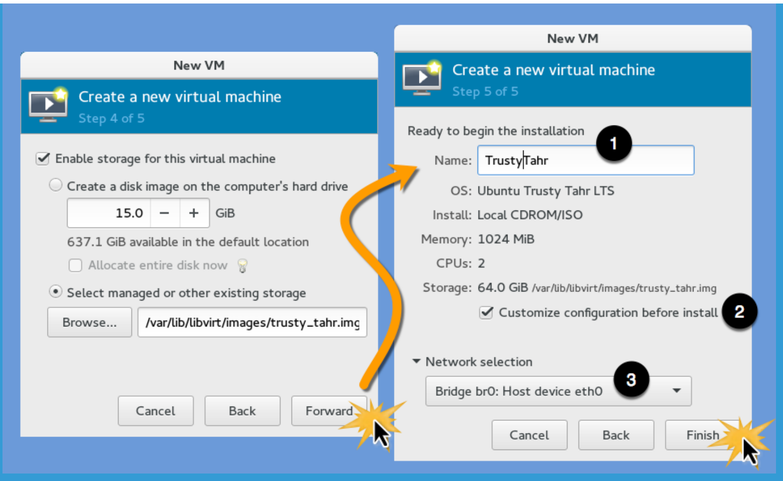
Πριν λίγο, πατώντας στο Browse για να επιλέξουμε το ISO image του Ubuntu, δεν εμφανίστηκε ένα τυπικό παράθυρο του file manager αλλά εκείνο που χρησιμοποιεί ο Virtual Machine Manager για τη διαχείριση των λεγόμενων pools. Ένα pool δεν είναι τίποτε άλλο από έναν τοπικό ή απομακρυσμένο χώρο αποθήκευσης. Σε ένα pool αποθηκεύουμε είτε ISO images λειτουργικών συστημάτων είτε τα αρχεία-εικονικούς δίσκους των VMs. Ανά πάσα στιγμή πρέπει να είναι ορισμένο τουλάχιστον ένα pool και σε κάθε pool επιτρέπεται να βρίσκονται αρχεία και των δύο κατηγοριών. Για λόγους καλής οργάνωσης, πάντως, τέτοια ανακατεμένα (και φρικαλέα) pools προτείνεται να τα αποφεύγουμε. Μετά την εγκατάσταση της υποδομής virtualization υπάρχει ορισμένο ακριβώς ένα pool, ονόματι default, το οποίο ουσιαστικά είναι ο κατάλογος /var/lib/libvirt/images του host. Το συγκεκριμένο pool εμείς το χρησιμοποιούμε αποκλειστικά για την αποθήκευση των εικονικών δίσκων των VMs. Παρεμπιπτόντως, σε ένα KVM VM είναι δυνατόν να δώσουμε απευθείας πρόσβαση σε διαμέρισμα φυσικού δίσκου ή σε ολόκληρο φυσικό δίσκο. Κατά τα αναμενόμενα, σ' αυτές τις περιπτώσεις δεν δημιουργείται κάποιο αρχείο, σε κανένα pool. Περισσότερα επί του θέματος θα δούμε αργότερα. Επιστρέφοντας στο προκείμενο, εκτός από το default εμείς χρησιμοποιούμε κι ένα pool που έχουμε ονομάσει Images. Σ' αυτό κρατάμε τα ISO images διαφόρων λειτουργικών συστημάτων που έχουμε κατεβάσει. Στην πραγματικότητα πρόκειται για τον κατάλογο ~/Downloads/Images, μέσα στον προσωπικό κατάλογο του χρήστη μας. Τώρα, για να ορίσουμε ένα νέο pool ξεκινάμε με κλικ στο κουμπάκι [+], κάτω αριστερά (1). Στο νέο παράθυρο που εμφανίζεται δίνουμε ένα όνομα για το νέο pool (θυρίδα Name), ενώ καθορίζουμε και τον τύπο του (επιλογή Type): για έναν τοπικό κατάλογο θέτουμε "Type = dir: Filesystem Directory". Πατάμε στο κουμπί Forward και με κλικ στο Browse (2) υποδεικνύουμε τη διαδρομή του τοπικού καταλόγου που αντιστοιχεί στο pool. Με κλικ στο Finish το παράθυρο Add a New Storage Pool κλείνει, και το όνομα του νέου pool εμφανίζεται στη σχετική λίστα του pool manager (3). Το pool φροντίζουμε ώστε να 'ναι επιλεγμένο, κι από το πλαίσιο δεξιά (4) διαλέγουμε το επιθυμητό ISO image. Πατάμε τέλος στο Choose Volume (5) κι έτσι καθορίζεται το ISO image από το οποίο θα γίνει η εγκατάσταση του guest OS για το VM μας.



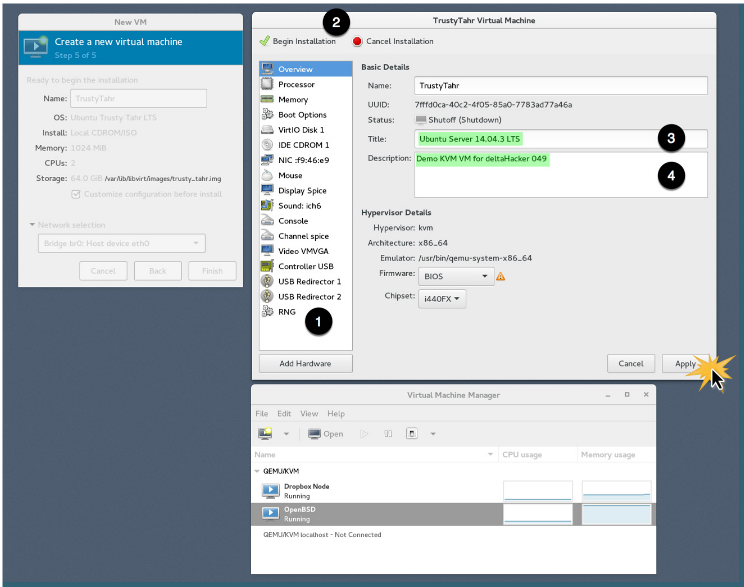
Αφού υποδείξαμε το ISO image του Ubuntu Server, παρατηρούμε ότι ο Virtual Machine Manager κατάφερε να θέσει σωστά, από μόνος του, τον τύπο και την έκδοση του guest OS (1). Στα επόμενα βήματα έχουμε την ευκαιρία να καθορίσουμε την ποσότητα της μνήμης RAM, καθώς και τον αριθμό των εικονικών επεξεργαστών του VM (2). Στη συνέχεια ασχολούμαστε με τον εικονικό ή τους εικονικούς δίσκους της μηχανής. Αρχικά, φροντίζουμε ώστε το Enable storage for this virtual machine να είναι τσεκαρισμένο. Είναι δυνατόν να δώσουμε εδώ, απευθείας, το μέγεθος του δίσκου, και ν' αφήσουμε τον Virtual Machine Manager να φροντίσει για τα υπόλοιπα (Create a disk image on the computer's hard drive). Αν όμως θέλουμε ν' αποκτήσουμε μια καλή εικόνα για τις δυνατότητες διαχείρισης storage που μας παρέχονται, επιλέγουμε το Select managed or other existing storage και κάνουμε ένα κλικ στο κουμπί Browse, από κάτω (3).



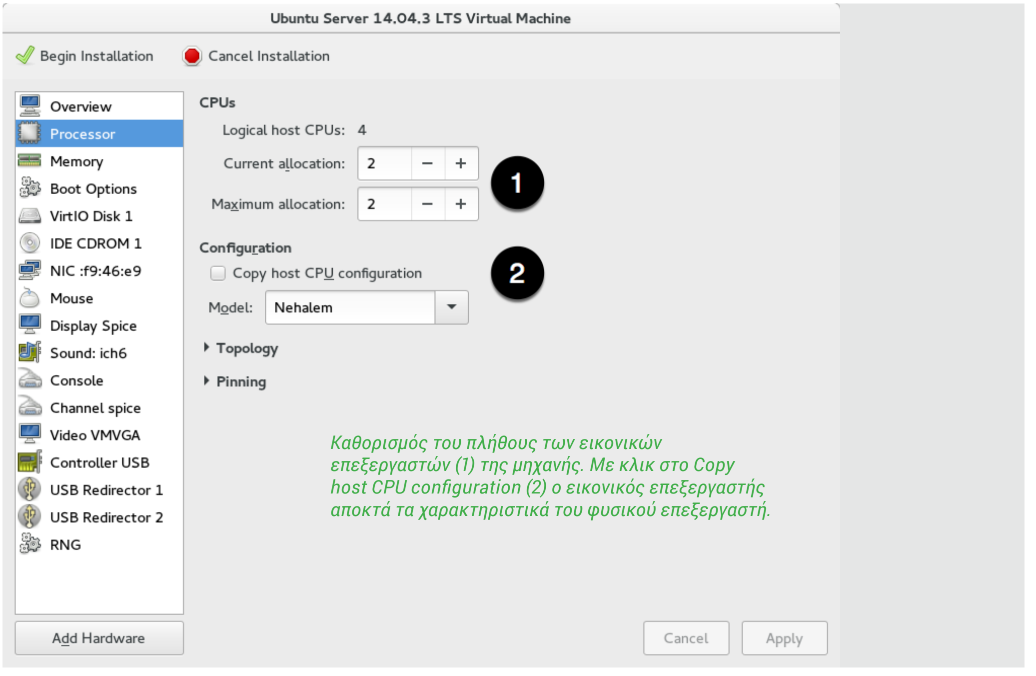
Για άλλη μια φορά ανοίγει το παράθυρο διαχείρισης των pools του Virtual Machine Manager. Για να φτιάξουμε τον εικονικό δίσκο της μηχανής επιλέγουμε το pool ονόματι default (1) και κάνουμε ένα κλικ στο κουμπάκι [+], στα δεξιά του Volumes (2). Θα ανοίξει ένα μικρό παράθυρο με τον τίτλο Add a Storage Volume. Στη θυρίδα Name δίνουμε το όνομα του αρχείου-εικονικού δίσκου κι από κάτω, στο Format, επιλέγουμε τον τύπο του (3). Ο προεπιλεγμένος τύπος για τα αρχεία-εικονικούς δίσκους είναι ο qcow2 και μεταξύ άλλων επιτρέπει τα snapshots, τη συμπίεση και την κρυπτογράφηση. Αν ενδιαφερόμαστε περισσότερο για τις επιδόσεις κι όχι για τις δυνατότητες, τότε ο τύπος raw είναι ό,τι πρέπει. Στη θυρίδα Max Capacity, εξάλλου, πληκτρολογούμε το μέγιστο επιθυμητό μέγεθος του εικονικού δίσκου, ενώ στην Allocation το αρχικό του μέγεθος (4). Στο παράδειγμά μας, λοιπόν, ο δίσκος ξεκινά με μηδενικό μέγεθος και μεγαλώνει όποτε κι όσο χρειάζεται, με άνω όριο τα 64GB. Φυσικά, για το guest OS ο δίσκος ανά πάσα στιγμή θα φαίνεται να έχει σταθερό μέγεθος (64GB). Αφού αποφασίσουμε για τις παραμέτρους του δίσκου και τις καθορίσουμε, κάνουμε ένα κλικ στο κουμπάκι Finish. Το αρχείο του εικονικού δίσκου θα εμφανιστεί στο κεντρικό πλαίσιο του διαχειριστή των pools (5). Τώρα, για να αντιστοιχιστεί στο VM τον επιλέγουμε κι αμέσως μετά πατάμε στο κουμπί Choose Volume, κάτω δεξιά.



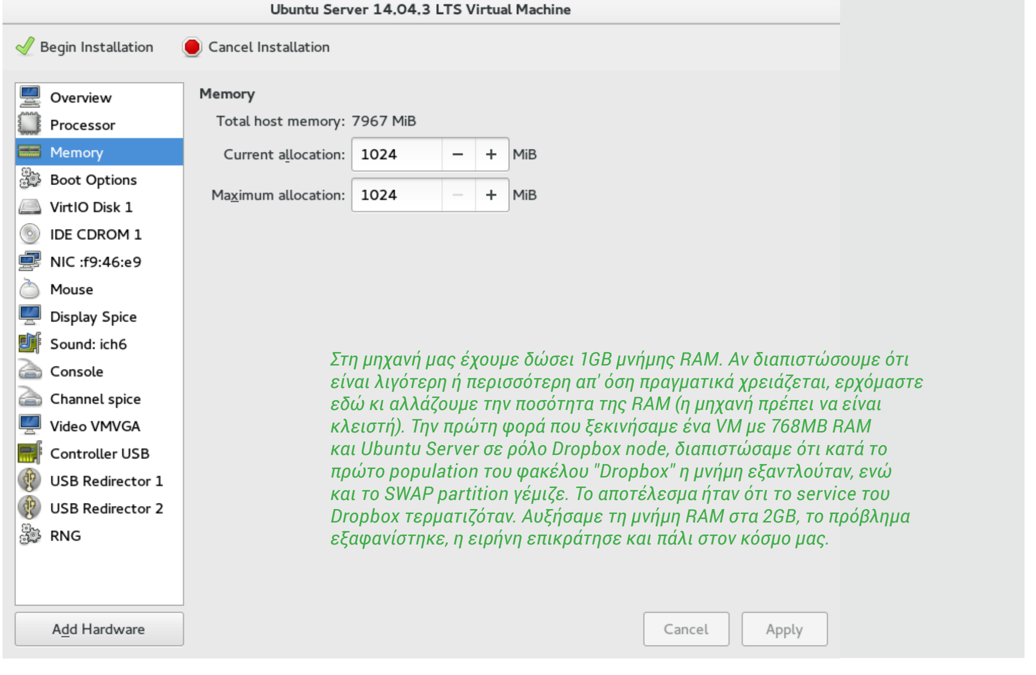
Βρισκόμαστε στο 4ο από τα 5 βήματα δημιουργίας VM και μόλις φτιάξαμε τον εικονικό δίσκο της μηχανής. Πατάμε στο κουμπί Forward και μεταβαίνουμε στο 5ο και τελευταίο βήμα. Στη θυρίδα Name δίνουμε ένα όνομα για τη μηχανή, χωρίς κενά (1). Τσεκάρουμε το Customize configuration before install (2), ώστε πριν ξεκινήσει η εγκατάσταση του guest OS να ρίξουμε μια τελευταία ματιά στο hardware του VM. Για τη δικτύωση του θέτουμε Network selection = Bridge br0: Host device eth0 (3), ώστε στην εικονική κάρτα Ethernet να αντιστοιχιστεί διεύθυνση IP από τον router του (αληθινού) εικονικού δικτύου. Τέλος, πατάμε στο κουμπί Finish.



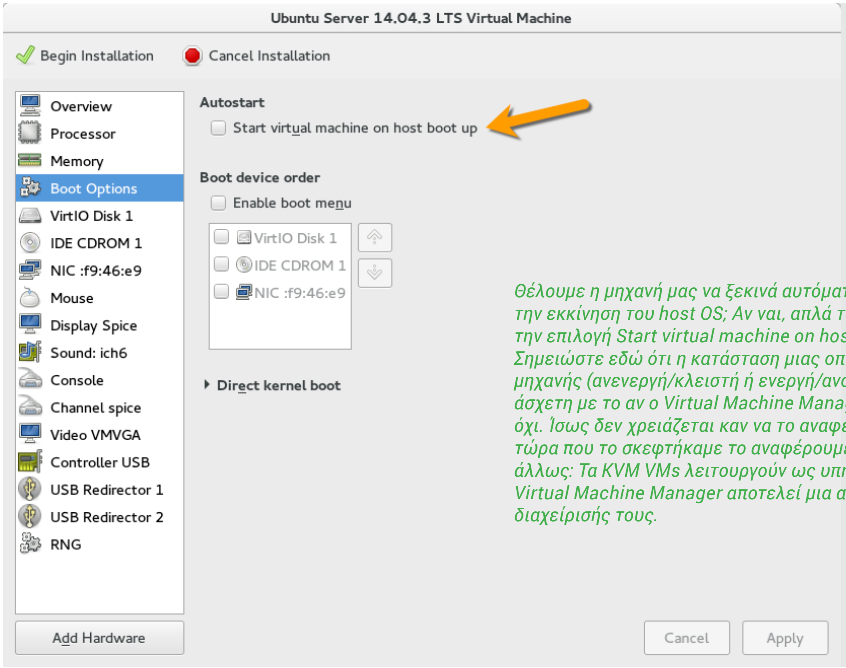
Σε κάθε εικονική μηχανή μάς παρέχεται λεπτομερής πρόσβαση στο υλικό που την απαρτίζει. Ο Virtual Machine Manager παρουσιάζει τα υποσυστήματα της επιλεγμένης μηχανής σε ένα κάθετο πλαίσιο στ' αριστερά (1). Όπως φανερώνει το κουμπί Add Hardware, κάτω από το εν λόγω πλαίσιο, είναι δυνατόν να προσθέτουμε υποσυστήματα, όπως, π.χ., εικονικούς δίσκους ή εικονικές κάρτες Ethernet, ακόμη και μετά τη συγκρότηση μιας μηχανής. Μπορούμε επίσης να επιλέγουμε υποσυστήματα και να τα αφαιρούμε. Για παράδειγμα, ένα VM σε ρόλο server μάλλον δεν χρειάζεται εικονική κάρτα ήχου. Καθώς εξετάζουμε τα υποσυστήματα της μηχανής μας –και με δεδομένο ότι μόλις τη φτιάξαμε και δεν έχει guest OS–, όταν είμαστε έτοιμοι πατάμε στο Begin Installation (2) και ξεκινά η εγκατάσταση του λειτουργικού συστήματος (του Ubuntu Server, στο πλαίσιο του παραδείγματός μας). Αλλά ας μην την ξεκινήσουμε αμέσως. Με κλικ πάνω σε κάθε γραμμή του κάθετου πλαισίου αριστερά, στη μεγαλύτερη περιοχή στα δεξιά εμφανίζονται όλες οι λεπτομέρειες που αφορούν στη μηχανή ή στο αντίστοιχο υποσύστημα. Από τη μεριά μας έχουμε δυνατότητα για επεμβάσεις και τροποποιήσεις. Με κλικ πάνω στο Overview, για παράδειγμα, μπορούμε να δώσουμε έναν χαρακτηριστικό τίτλο (3) καθώς και μια λεπτομερή περιγραφή για τη μηχανή (4). Όταν έχουμε λίγα μόνο VMs τέτοιες πληροφορίες δεν φαίνεται να 'χουν μεγάλη αξία, αυτό όμως αλλάζει καθώς δημιουργούμε νέες μηχανές. Κάθε επέμβαση που πραγματοποιούμε την παγιώνουμε με κλικ στο κουμπί Apply, κάτω δεξιά.



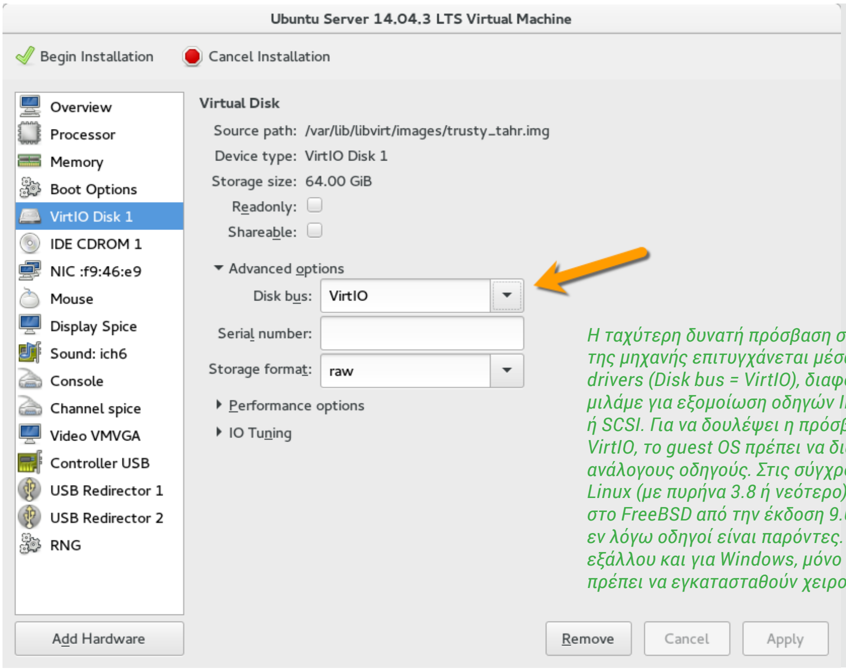
Καθορισμός του πλήθους των εικονικών επεξεργαστών (1) της μηχανής. Με κλικ στο Copy host CPU configuration (2) ο εικονικός επεξεργαστής αποκτά τα χαρακτηριστικά του φυσικού επεξεργαστή.



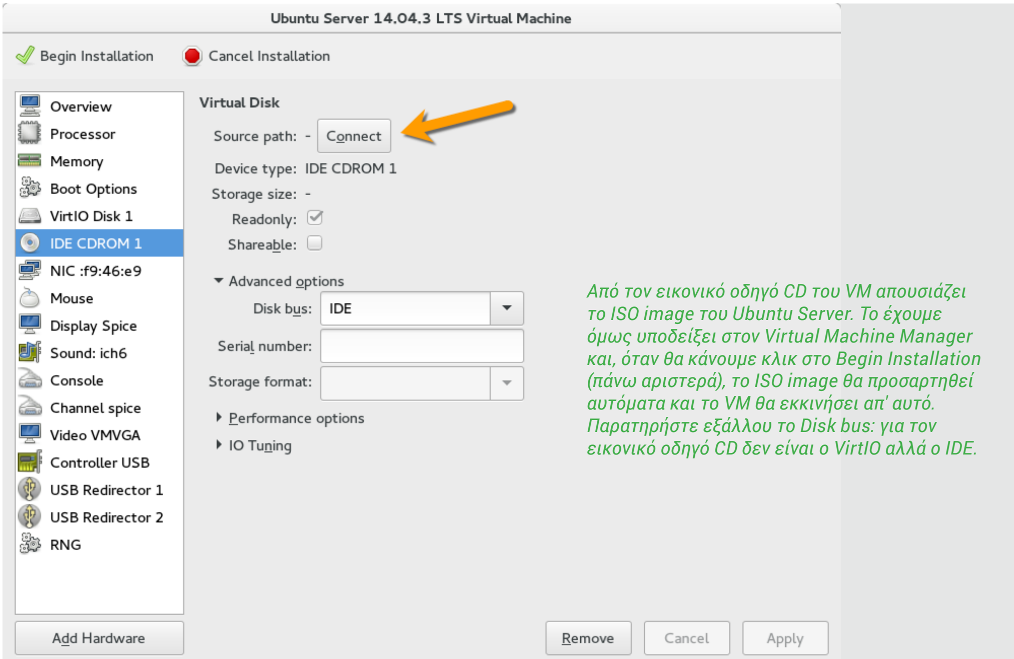
Στη μηχανή μας έχουμε δώσει 1GB μνήμης RAM. Αν διαπιστώσουμε ότι είναι λιγότερη ή περισσότερη απ' όση πραγματικά χρειάζεται, ερχόμαστε εδώ κι αλλάζουμε την ποσότητα της RAM (η μηχανή πρέπει να είναι κλειστή). Την πρώτη φορά που ξεκινήσαμε ένα VM με 768MB RAM και Ubuntu Server σε ρόλο Dropbox node, διαπιστώσαμε ότι κατά το πρώτο population του φακέλου "Dropbox" η μνήμη εξαντλούταν, ενώ και το SWAP partition γέμιζε. Το αποτέλεσμα ήταν ότι το service του Dropbox τερματιζόταν. Αυξήσαμε τη μνήμη RAM στα 2GB, το πρόβλημα εξαφανίστηκε, η ειρήνη επικράτησε και πάλι στον κόσμο μας.



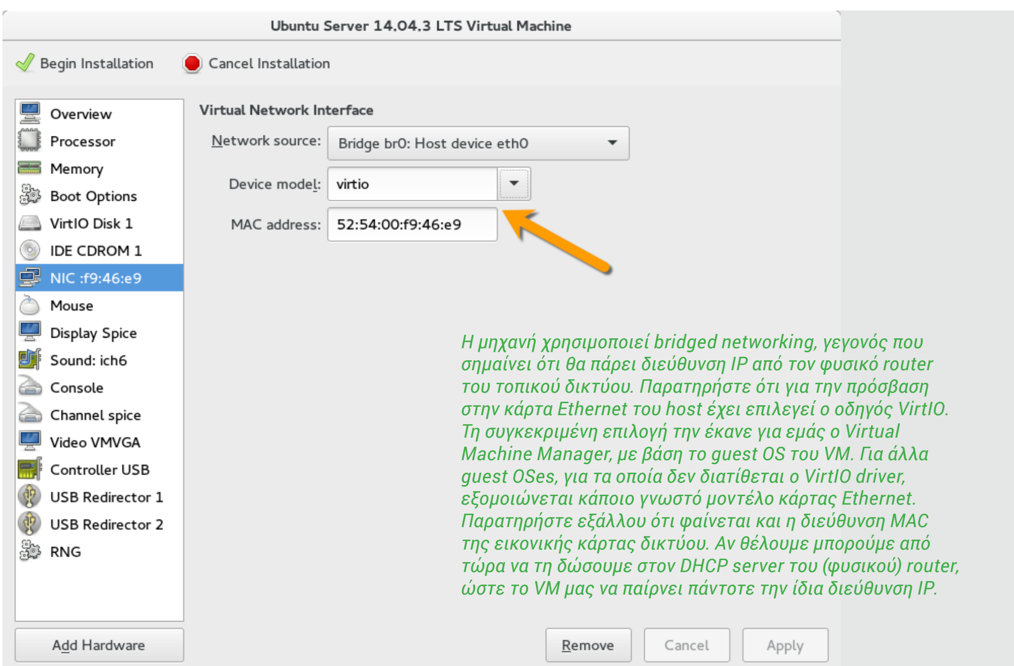
Θέλουμε η μηχανή μας να ξεκινά αυτόματα, κατά την εκκίνηση του host OS; Αν ναι, απλά τσεκάρουμε την επιλογή Start virtual machine on host boot up. Σημειώστε εδώ ότι η κατάσταση μιας οποιασδήποτε μηχανής (ανενεργή/κλειστή ή ενεργή/ανοικτή) είναι άσχετη με το αν ο Virtual Machine Manager τρέχει ή όχι. Ίσως δεν χρειάζεται καν να το αναφέρουμε, αλλά τώρα που το σκεφτήκαμε το αναφέρουμε ούτως ή άλλως: Τα KVM VMs λειτουργούν ως υπηρεσίες, ενώ ο Virtual Machine Manager αποτελεί μια απλή εφαρμογή διαχείρισής τους.



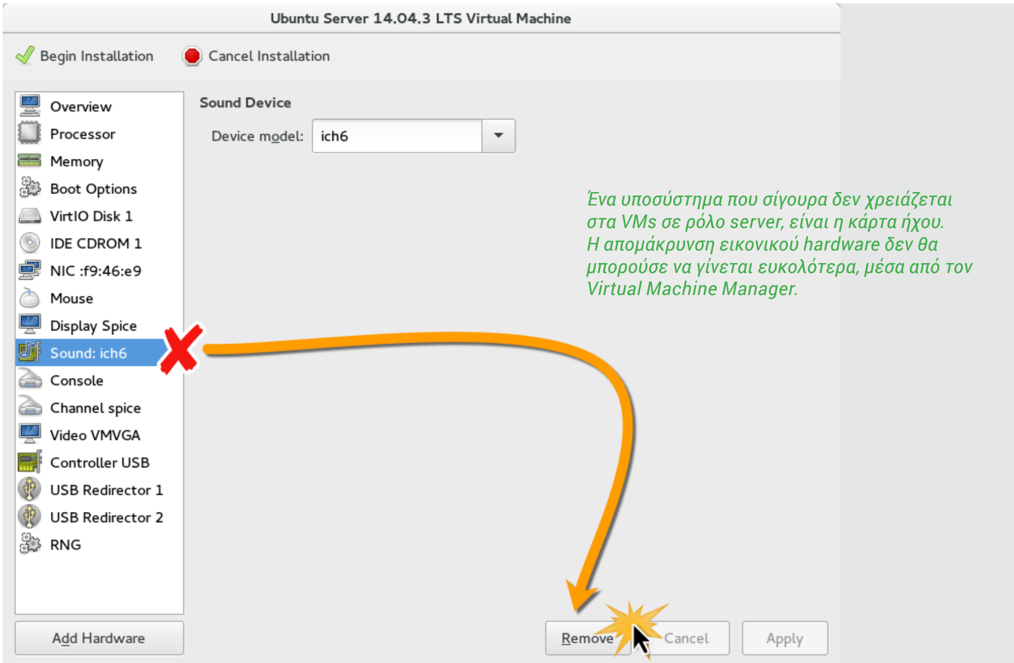
Η ταχύτερη δυνατή πρόσβαση στο δίσκο της μηχανής επιτυγχάνεται μέσω των VirtIO drivers (Disk bus = VirtIO), διαφορετικά μιλάμε για εξομοίωση οδηγών IDE, SATA ή SCSI. Για να δουλέψει η πρόσβαση μέσω VirtIO, το guest OS πρέπει να διαθέτει τους ανάλογους οδηγούς. Στις σύγχρονες διανομές Linux (με πυρήνα 3.8 ή νεότερο) καθώς και στο FreeBSD από την έκδοση 9.0 και μετά, οι εν λόγω οδηγοί είναι παρόντες. Διατίθενται εξάλλου και για Windows, μόνο που εκεί πρέπει να εγκατασταθούν χειροκίνητα.



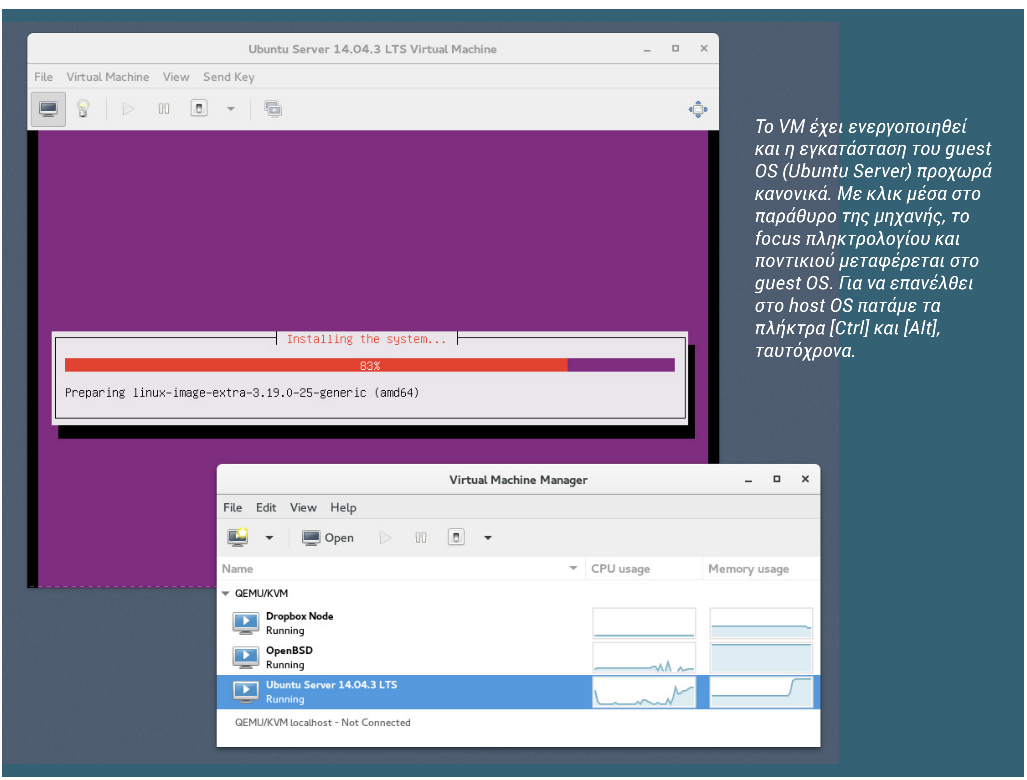
Από τον εικονικό οδηγό CD του VM απουσιάζει το ISO image του Ubuntu Server. Το έχουμε όμως υποδείξει στον Virtual Machine Manager και, όταν θα κάνουμε κλικ στο Begin Installation (πάνω αριστερά), το ISO image θα προσαρτηθεί αυτόματα και το VM θα εκκινήσει απ' αυτό. Παρατηρήστε εξάλλου το Disk bus: για τον εικονικό οδηγό CD δεν είναι ο VirtIO αλλά ο IDE.



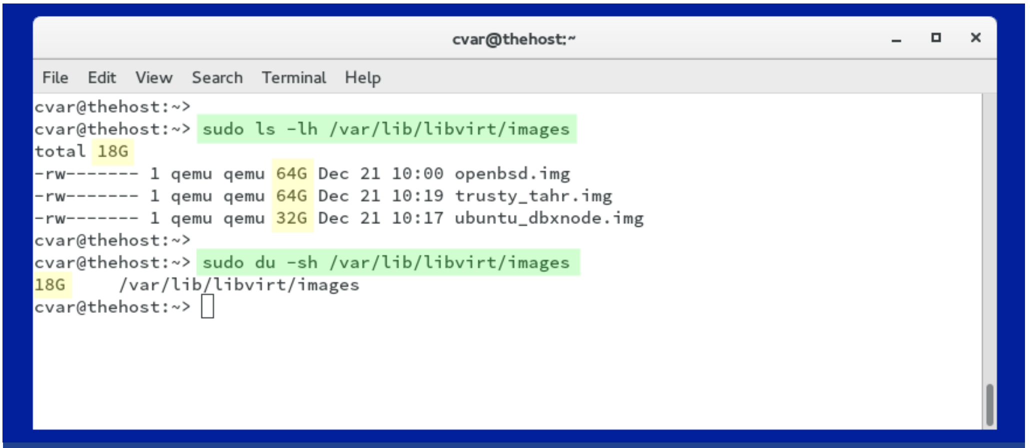
Η μηχανή χρησιμοποιεί bridged networking, γεγονός που σημαίνει ότι θα πάρει διεύθυνση IP από τον φυσικό router του τοπικού δικτύου. Παρατηρήστε ότι για την πρόσβαση στην κάρτα Ethernet του host έχει επιλεγεί ο οδηγός VirtIO. Τη συγκεκριμένη επιλογή την έκανε για εμάς ο Virtual Machine Manager, με βάση το guest OS του VM. Για άλλα guest OSes, για τα οποία δεν διατίθεται ο VirtIO driver, εξομοιώνεται κάποιο γνωστό μοντέλο κάρτας Ethernet. Παρατηρήστε εξάλλου ότι φαίνεται και η διεύθυνση MAC της εικονικής κάρτας δικτύου. Αν θέλουμε μπορούμε από τώρα να τη δώσουμε στον DHCP server του (φυσικού) router, ώστε το VM μας να παίρνει πάντοτε την ίδια διεύθυνση IP.



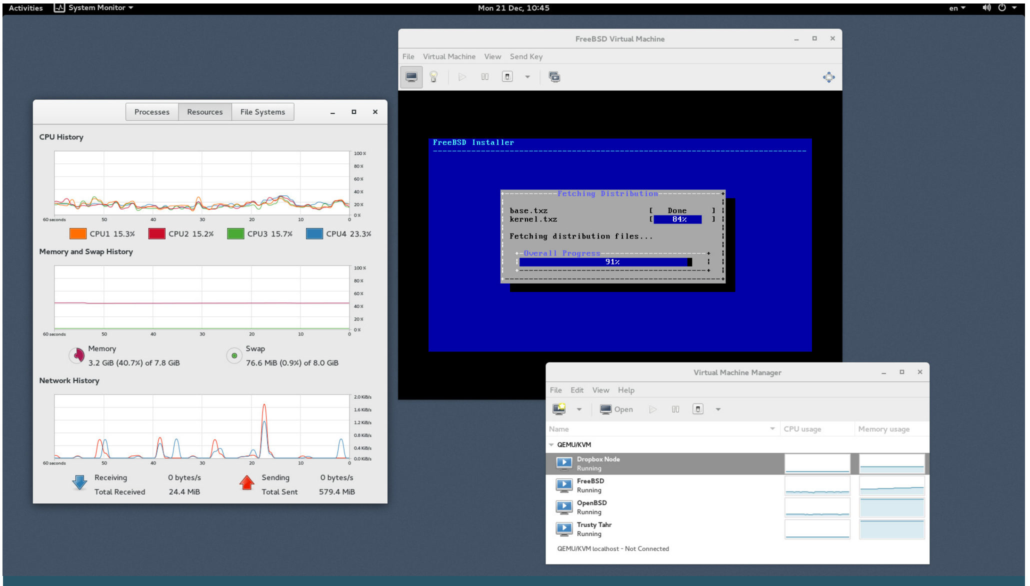
Ένα υποσύστημα που σίγουρα δεν χρειάζεται στα VMs σε ρόλο server, είναι η κάρτα ήχου. Η απομάκρυνση εικονικού hardware δεν θα μπορούσε να γίνεται ευκολότερα, μέσα από τον Virtual Machine Manager.



Το VM έχει ενεργοποιηθεί και η εγκατάσταση του guest OS (Ubuntu Server) προχωρά κανονικά. Με κλικ μέσα στο παράθυρο της μηχανής, το focus πληκτρολογίου και ποντικιού μεταφέρεται στο guest OS. Για να επανέλθει στο host OS πατάμε τα πλήκτρα [Ctrl] και [Alt], ταυτόχρονα.



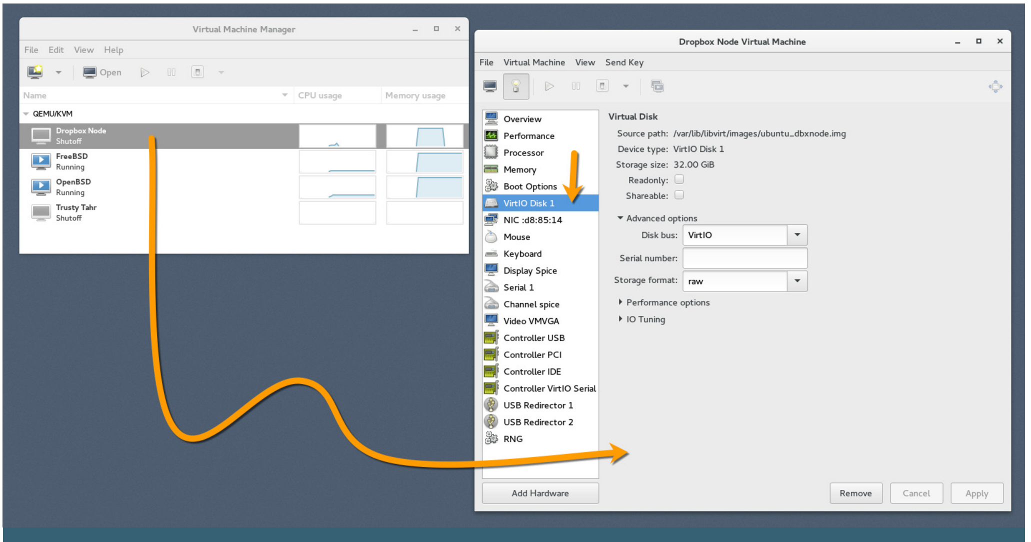
Από ένα παράθυρο τερματικού ρίχνουμε μια ματιά στον κατάλογο /var/lib/libvirt/images, στον οποίο εξ ορισμού κατοικούν οι εικονικοί δίσκοι των VMs. Βλέπουμε τρία αρχεία και τα αντίστοιχα μεγέθη τους. Συνολικά, τα αρχεία μέσα στον images θα έπρεπε να έχουν μέγεθος 64+64+32 = 160 gigabytes. Στην πραγματικότητα, όμως, τη στιγμή που ελήφθη το screenshot καταλάμβαναν μόλις 18GB. Αυτά είναι τα καλά των εικονικών δίσκων, που μεγαλώνουν δυναμικά!



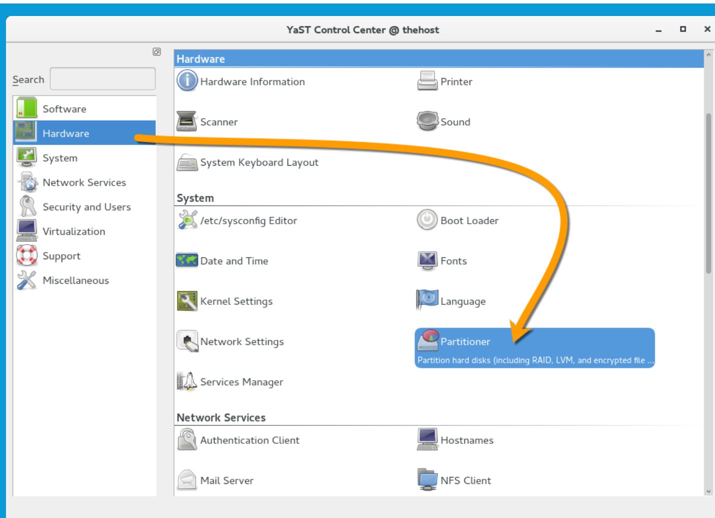
Μετά την εγκατάσταση του Ubuntu Server (Trusty Tahr) μάς άνοιξε η όρεξη και είπαμε να φτιάξουμε άλλο ένα VM, με το αγαπημένο μας FreeBSD. Τη στιγμή του screenshot υπήρχαν τέσσερα VMs ενεργά και, όπως βλέπετε κι από το System Monitor του GNOME, το host computer δεν ζοριζόταν ιδιαίτερα.

Αντιστοίχιση φυσικού δίσκου σε VM

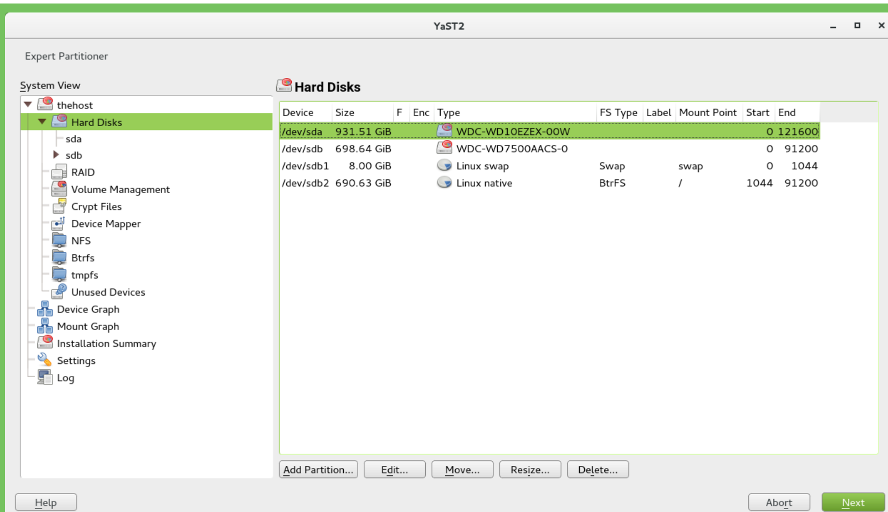
Μερικές φορές, κι αναλόγως του ρόλου που έχει μια εικονική μηχανή, είναι χρήσιμο να της δίνουμε αληθινούς (φυσικούς) δίσκους ή διαμερίσματα αληθινών δίσκων. Αυτό αποφασίσαμε να κάνουμε για ένα KVM VM με Ubuntu Server, που χρησιμοποιούμε ως Dropbox node. Τι εννοούμε; Θα σας πούμε αμέσως. Διαθέτουμε λογαριασμό Dropbox Pro τους ενός terabyte, ο οποίος αυτή τη στιγμή έχει γύρω στα 270GB. Όλον αυτόν τον όγκο των δεδομένων δεν τον θέλουμε στον SSD του laptop, χωρητικότητας 512GB, θέλουμε ωστόσο ένα τοπικό μηχάνημα το οποίο ανά πάσα στιγμή θα έχει *όλα* τα δεδομένα που βρίσκονται online, στο Dropbox μας. Στο σχετικό VM θα μπορούσαμε να δώσουμε έναν εικονικό δίσκο με άνω όριο μεγέθους το 1TB. Ένα τέτοιο αρχείο όμως δεν θα ήταν και πολύ βολικό, ειδικά αν επρόκειτο να μεταφερθεί σε διαφορετικό φυσικό host. Αγοράσαμε, λοιπόν, έναν φυσικό δίσκο του 1TB, το προσθέσαμε στο host computer και στη συνέχεια τον δώσαμε *απευθείας* στο KVM VM. Χάρη σ' αυτή τη διευθέτηση, στα δεδομένα του δίσκου έχει πρόσβαση το VM αλλά *και* το host computer. Επίσης, μπορεί να έχει πρόσβαση κι οποιοσδήποτε άλλος host με Linux – αρκεί να μεταφέρουμε εκεί τον δίσκο. Στο υπόλοιπο του άρθρου δείχνουμε πώς αντιστοιχίσαμε στο VM τον φυσικό μας δίσκο.



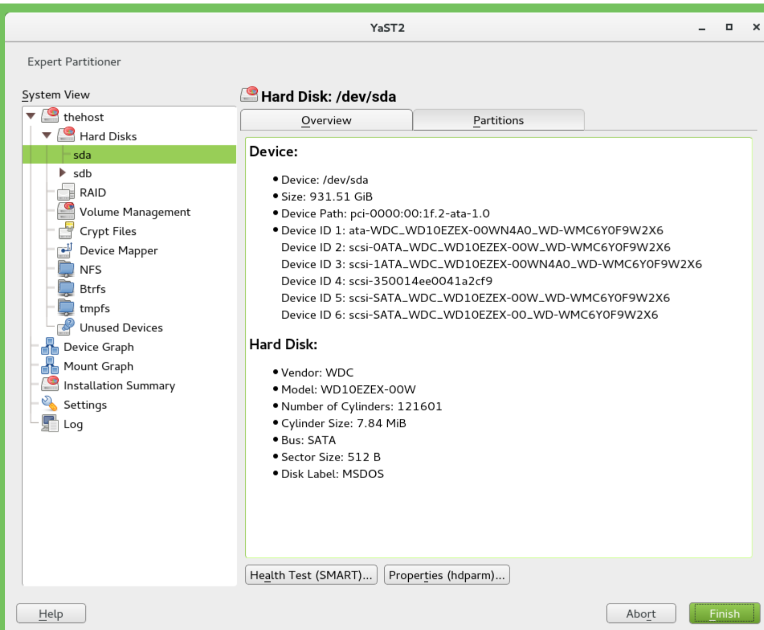
Το VM στο οποίο θα δώσουμε τον φυσικό δίσκο ονομάζεται "Dropbox Node" και, όπως βλέπουμε από τον Virtual Machine Manager, αυτή τη στιγμή είναι κλειστό. Θα παραμείνει έτσι και θα το ξεκινήσουμε αφού προσθέσουμε το δίσκο. Από τις ιδιότητες της μηχανής παρατηρούμε ότι το VM προς το παρόν διαθέτει έναν εικονικό δίσκο, μεγέθους 32GB. Πρόκειται για το δίσκο εγκατάστασης του λειτουργικού συστήματος (Ubuntu Server) και φυσικά για το δίσκο εκκίνησης της μηχανής.



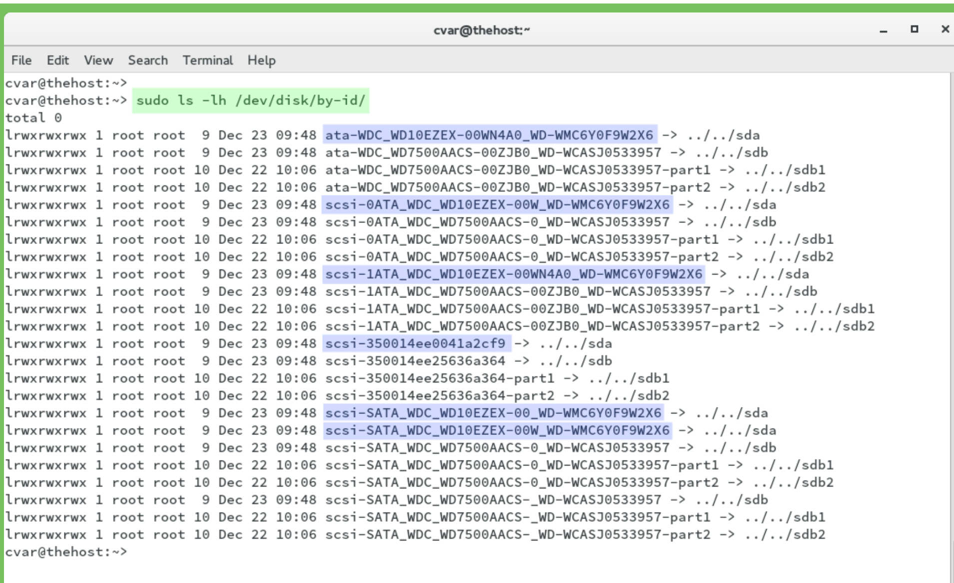
Στο φυσικό σύστημα με το openSUSE τρέχουμε το YaST κι ενεργοποιούμε το module ονόματι Partitioner (βρίσκεται στην κατηγορία Hardware).



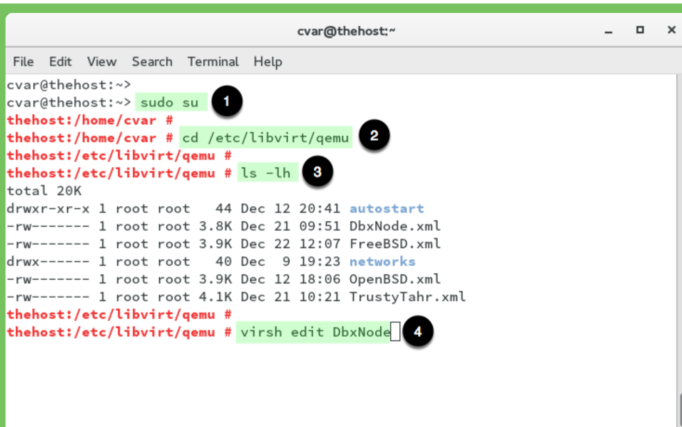
Στο αριστερό κάθετο πλαίσιο του Partitioner, με τίτλο System View, αναπτύσσουμε το δέντρο δίνοντας thehost → Hard Disks (το δικό σας σύστημα πιθανώς θα έχει διαφορετικό hostname). Παρατηρούμε ότι το Linux έχει εντοπίσει κι ονομάσει δύο σκληρούς δίσκους, τον sda και τον sdb. Δείτε και το μεγαλύτερο πλαίσιο, με όνομα Hard Disks, στα δεξιά. Στο παράδειγμά μας ο δίσκος sdb έχει δύο διαμερίσματα (partitions): το sdb1 (τύπου Swap) και το sdb2 (τύπου BtrFS). Προφανώς, ο δίσκος sdb είναι εκείνος στον οποίο έχει εγκατασταθεί το openSUSE μας. Ο δε δίσκος sda στερείται διαμερισμάτων κι έχει μέγεθος κοντά στο 1TB. Αυτός ακριβώς είναι ο νέος μας δίσκος, τον οποίο θέλουμε να δώσουμε στο VM με το Ubuntu Server (δηλαδή στο Dropbox Node). Το device name της συσκευής, σύμφωνα με το openSUSE, είναι το /dev/sda. Το θέμα εδώ είναι ότι το συγκεκριμένο όνομα παράγεται δυναμικά κι ενδέχεται ν' αλλάξει, π.χ., αν βάλουμε το δίσκο σε διαφορετικό port πάνω στη μητρική του PC ή τον μεταφέρουμε σε άλλο PC. Το VM μας, λοιπόν, δεν είναι έξυπνο ν' αναφέρεται στον φυσικό δίσκο με βάση το δυναμικό του όνομα. Ευτυχώς, κάθε κατασκευαστής αντιστοιχίζει στους δίσκους κάποια ονόματα που μένουν αναλλοίωτα και δεν εξαρτώνται από το port στο οποίο συνδέεται η συσκευή, ούτε από το εκάστοτε λειτουργικό σύστημα.



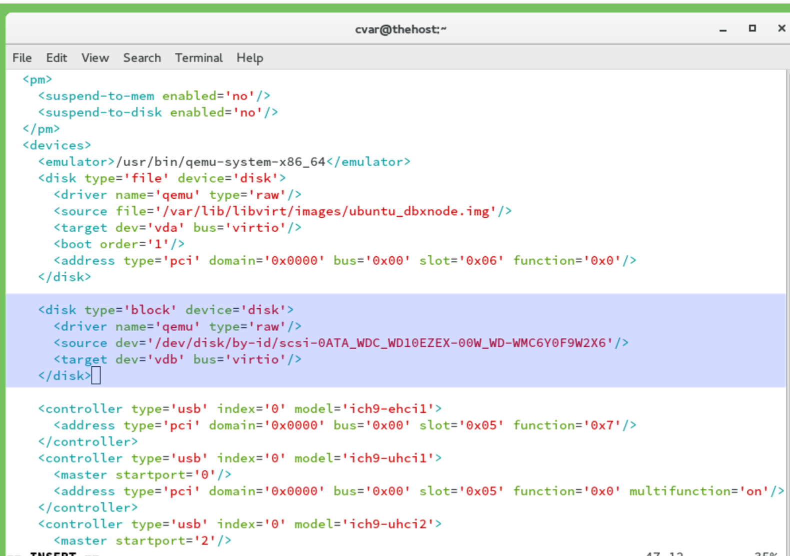
Για να δούμε τα στατικά ονόματα του δίσκου μας, στο πλαίσιο System View του Partitioner κάνουμε απλά ένα κλικ στο όνομα της συσκευής κατά Linux (sda). Αμέσως, στο πλαίσιο δεξιά εμφανίζονται πληροφορίες που αφορούν στο δίσκο και μεταξύ αυτών είναι και τα "σταθερά" ονόματά του. Πρόκειται για όλα αυτά τα "Device ID" και είναι έξι στο πλήθος. Ένα οποιοδήποτε εξ αυτών μας κάνει – κι εμείς εστιάσαμε στο Device ID 2.



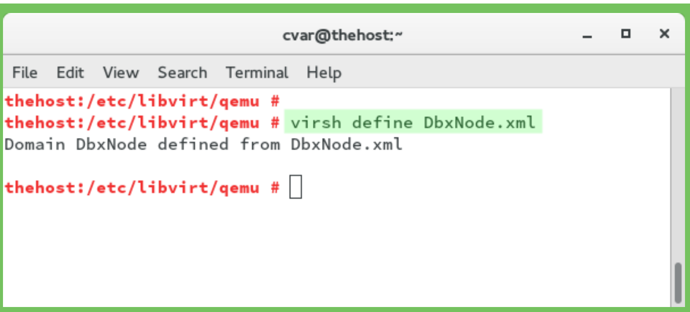
Χωρίς το YaST και τον Partitioner, τα Device IDs τα βλέπουμε και μέσα στον κατάλογο /dev/disk/by-id. Όλα τα Device IDs που μας ενδιαφέρουν αποτελούν symbolic links προς το όνομα που έχει αποδώσει το Linux στο δίσκο (sda).



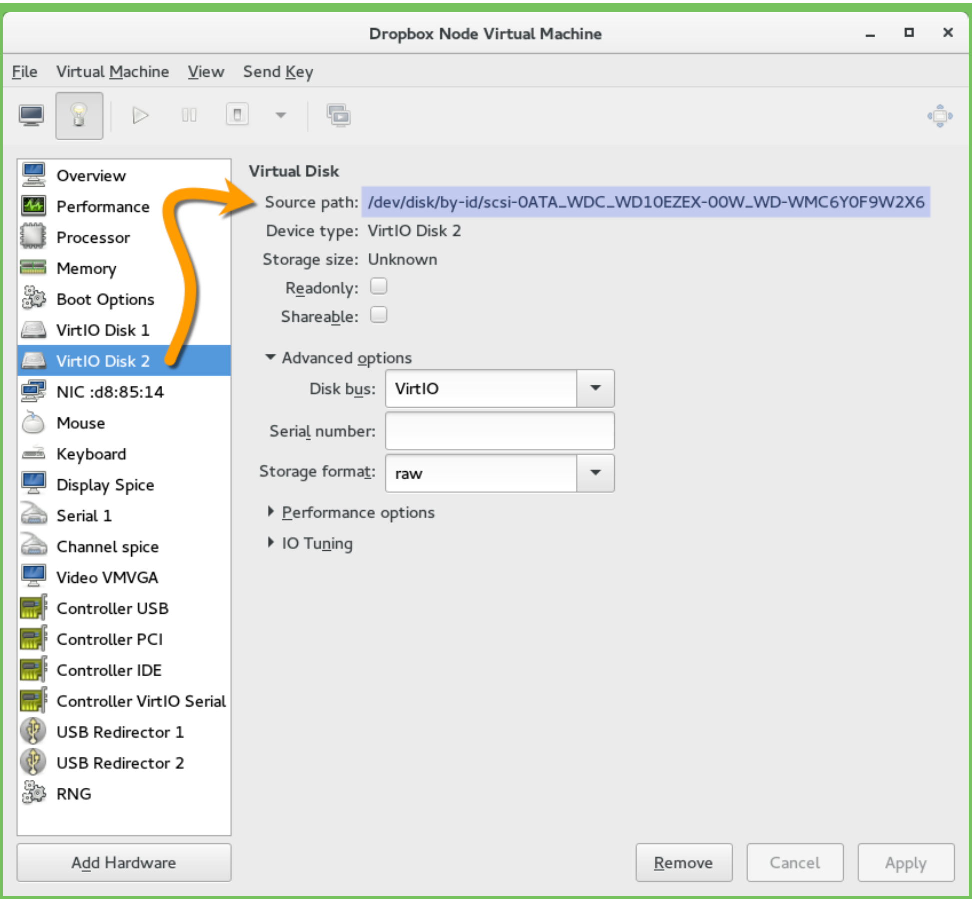
Προκειμένου να ενημερώσουμε το VM μας για την παρουσία του φυσικού δίσκου, στον οποίο θέλουμε να έχει απευθείας πρόσβαση, δεν εργαζόμαστε μέσα από τον Virtual Machine Manager. Αντίθετα, κάνουμε συγκεκριμένες προσθήκες στο αρχείο XML που περιγράφει τις ιδιότητες της εικονικής μηχανής. Ανοίγουμε ένα τερματικό κι αποκτούμε δικαιώματα root (1). Μεταβαίνουμε στον κατάλογο /etc/libvirt/qemu (2), αφού σ' αυτόν διατηρούνται τα αρχεία XML των μηχανών. Βλέποντας τα περιεχόμενα του καταλόγου (3), εύκολα διακρίνουμε το αρχείο στο οποίο πρέπει να επέμβουμε. Για εμάς είναι το DbxNode.xml. Προσέξτε, όμως: Αντί να το ανοίξουμε απευθείας με κάποιον text editor πληκτρολογούμε κάτι σαν "virsh edit DbxNode" (χωρίς τα εισαγωγικά και χωρίς την κατάληξη του αρχείου).



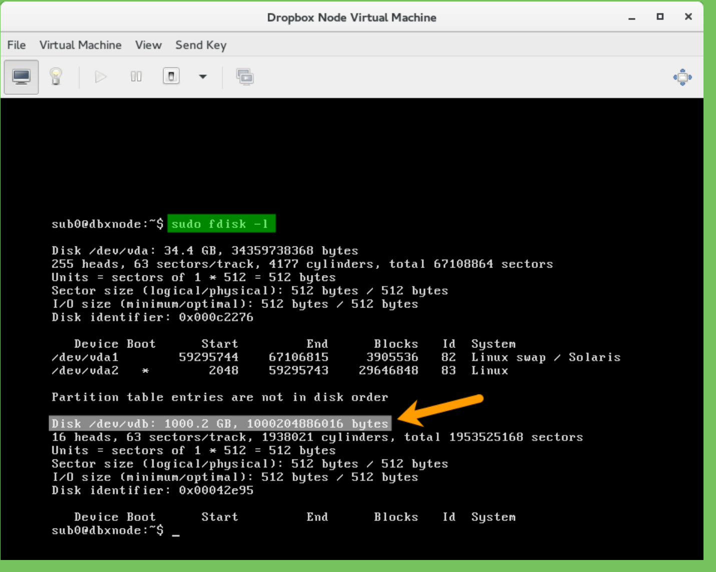
Η εντολή που μόλις δώσαμε ανοίγει το αρχείο DbxNode.xml μέσα από το vi, τον προκαθορισμένο text editor στο openSUSE. Αν δεν είστε εξοικειωμένοι με τον εν λόγω editor κάλλιστα μπορούμε να τον αλλάξουμε, αφού όμως πρώτα τον εγκαταλείψουμε πατώντας [Shift]+[;], γράφοντας "q!" (χωρίς τα εισαγωγικά) και δίνοντας ένα [Enter]. Ένας εύχρηστος και κατά την άποψη του γράφοντα πολύ πιο φιλικός editor, είναι το nano. Σε περίπτωση που δεν είναι εγκατεστημένο στο openSUSE σας, γράψτε "zypper install nano" και μετά πληκτρολογήστε EDITOR="/usr/bin/nano" virsh edit DbxNode. Όποιος κι αν είναι ο editor, πηγαίνουμε στην ενότητα devices και προσθέτουμε ένα νέο disk μπλοκ, κάτω από το υπάρχον και σαν αυτό που είναι τονισμένο στο screenshot. Προφανώς, το μόνο που θα αλλάξει για τη δική σας περίπτωση είναι το Device ID στη γραμμή <source dev='dev/disk/by-id/...'/>. Επίσης, αν το VM σας έχει δύο δίσκους, τότε αυτό το vdb στη γραμμή <target dev='dvb' bus='virtio'/> θα πρέπει να αντικατασταθεί με το vdc. Μετά την προσθήκη του νέου disk μπλοκ στο DbxNode.xml, αποθηκεύουμε τις αλλαγές κι εγκαταλείπουμε τον editor. (Αν χρησιμοποιούμε το nano, δίνουμε [CTRL+O] κι [Enter] για αποθήκευση και μετά ένα [CTRL+X] για έξοδο.)



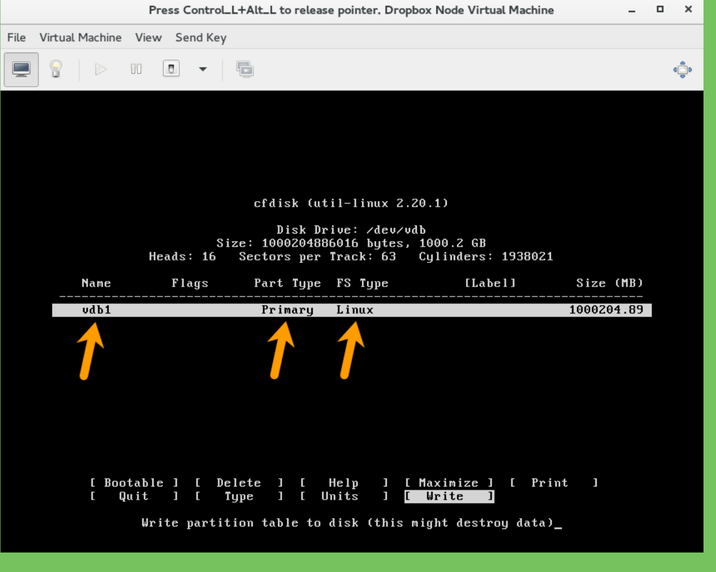
Η προσθήκη που κάναμε στο DbxNode.xml δεν θα ληφθεί υπόψη αν δεν πληκτρολογήσουμε και "virsh define DbxNode.xml" (ναι, αυτή τη φορά με την κατάληξη). Αν δεν έχουμε κάνει κάποιο λάθος, θα πρέπει να πάρουμε ένα μήνυμα σαν αυτό που απεικονίζεται στο screenshot.



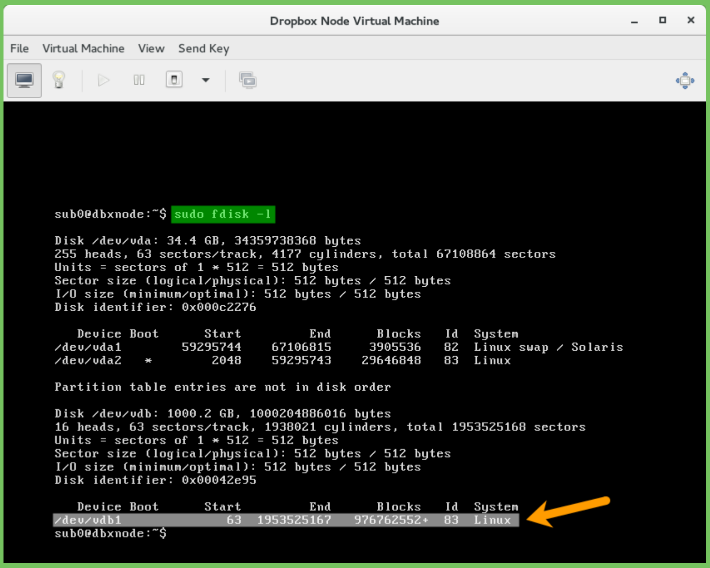
Το μήνυμα που πήραμε στο τερματικό δεν μας αρκεί για να βεβαιωθούμε ότι ο δίσκος έχει προστεθεί στο VM. Μέσα από τον Virtual Machine Manager, λοιπόν, ρίχνουμε μια ματιά στις ιδιότητες της μηχανής (για το παράδειγμά μας, εκείνης με όνομα Dropbox Node). Λογικά, τώρα θα έχει δύο δίσκους. Ο δεύτερος (VirtIO Disk 2) είναι ο φυσικός δίσκος που μόλις προσθέσαμε. Δείτε το Source path και θα πειστείτε.



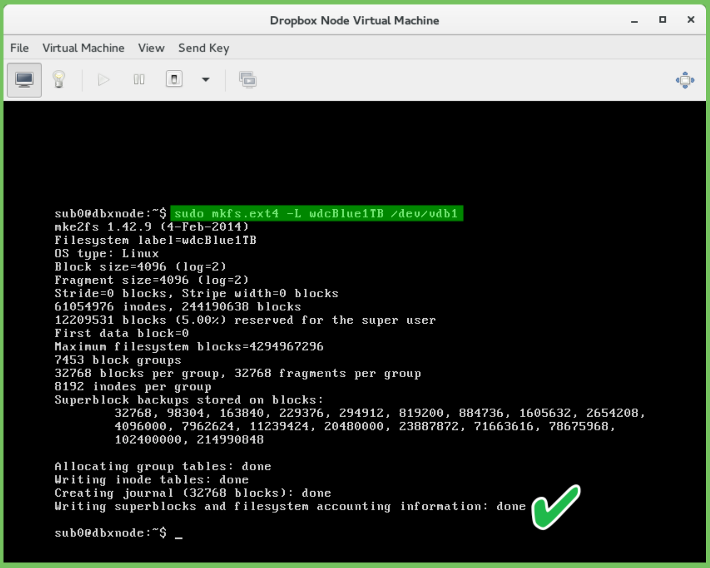
Εντάξει, ο καλύτερος τρόπος για να βεβαιωθούμε ότι το VM βλέπει το φυσικό δίσκο, είναι να ενεργοποιήσουμε τη μηχανή και να δούμε από μόνοι μας. Στο στιγμιότυπο έχουμε ξεκινήσει το Ubuntu Server KVM VM και με τη βοήθεια του fdisk διαπιστώνουμε ότι, πράγματι, ο δίσκος είναι ορατός από το guest OS.



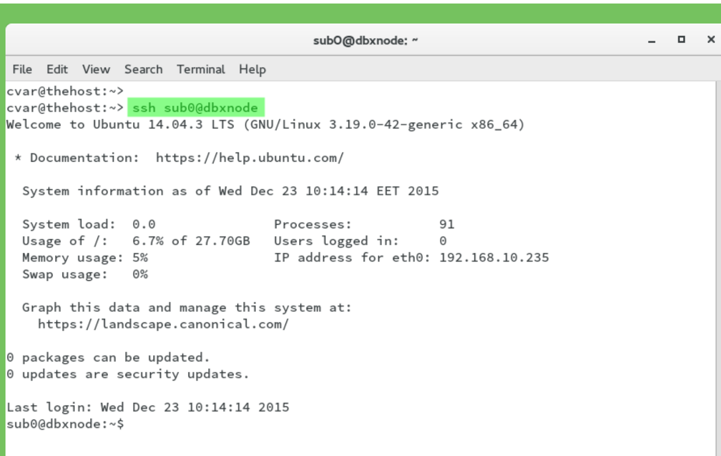
Προκειμένου να χρησιμοποιήσουμε το δίσκο, πρέπει να φτιάξουμε τουλάχιστον ένα διαμέρισμα πάνω του. Προς τούτο καταφεύγουμε στο εργαλείο cfdisk (στην κονσόλα πληκτρολογούμε "sudo cfdisk /dev/vdb") και δημιουργούμε ακριβώς ένα διαμέρισμα, το οποίο καταλαμβάνει όλο το διαθέσιμο χώρο.



Αφού εγκαταλείψουμε το cfdisk βεβαιωνόμαστε ότι το νέο διαμέρισμα είναι παρόν, πληκτρολογώντας "sudo fdisk -l". Στο παράδειγμά μας, το device του νέου διαμερίσματος είναι το /dev/dvb1.



Σειρά έχει το format του partition, μ' άλλα λόγια η δημιουργία συστήματος αρχείων (filesystem) για το /dev/dvb1. Το σύστημα αρχείων Ext4 είναι μια χαρά για τις ανάγκες μας και το δημιουργούμε όπως υποδεικνύεται στο στιγμιότυπο (αυτό το "wdcBlue1TB" είναι το label που επιλέξαμε να δώσουμε στο διαμέρισμα).



```
sub0@dbxnode: ~
File  Edit  View  Search  Terminal  Help
cvar@thehost:~>
cvar@thehost:~> ssh sub0@dbxnode
Welcome to Ubuntu 14.04.3 LTS (GNU/Linux 3.19.0-42-generic x86_64)

 * Documentation:  https://help.ubuntu.com/

  System information as of Wed Dec 23 10:14:14 EET 2015

  System load:  0.0                Processes:           91
  Usage of /:   6.7% of 27.70GB    Users logged in:     0
  Memory usage: 5%                 IP address for eth0: 192.168.10.235
  Swap usage:   0%

  Graph this data and manage this system at:
    https://landscape.canonical.com/

0 packages can be updated.
0 updates are security updates.

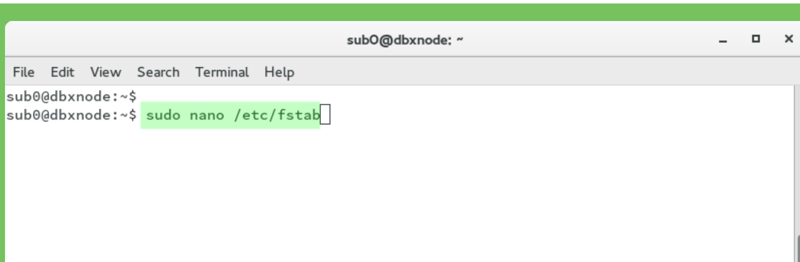
Last login: Wed Dec 23 10:14:14 2015
sub0@dbxnode:~$
```

*Για τη συνέχεια, επειδή θα θέλουμε να αντιγράψουμε *εύκολα* το UUID του νέου διαμερίσματος και να το επικολλήσουμε στο /etc/fstab, αφήνουμε την κονσόλα του Virtual Machine Manager κι από ένα τερματικό του openSUSE κάνουμε SSH login στο Dropbox Node. Ο λογαριασμός του χρήστη στο παράδειγμά μας, στον οποίο κάνουμε SSH login, έχει ως username το sub0. Χάρη εξάλλου στο pfSense box μπροστά από το KVM VM με το Ubuntu Server, αντί να πληκτρολογήσουμε τη διεύθυνση IP του VM γράψαμε, απλά, dbxnode (αυτό είναι το hostname του).*



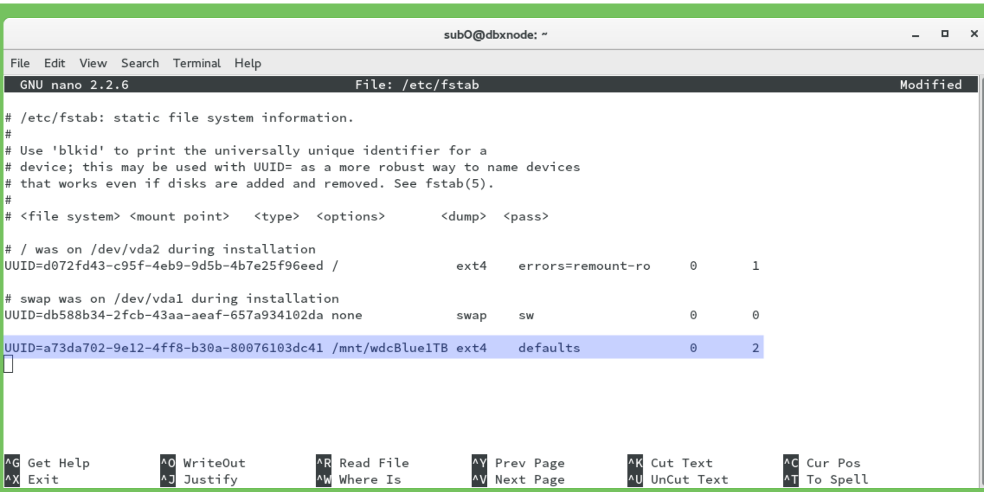
```
sub0@dbxnode: ~
File  Edit  View  Search  Terminal  Help
sub0@dbxnode:~$
sub0@dbxnode:~$ ls -lh /dev/disk/by-uuid/
total 0
lrwxrwxrwx 1 root root 10 Dec 23 10:18 a73da702-9e12-4ff8-b30a-80076103dc41 -> ../../vdb1
lrwxrwxrwx 1 root root 10 Dec 23 10:14 d072fd43-c95f-4eb9-9d5b-4b7e25f96eed -> ../../vda2
lrwxrwxrwx 1 root root 10 Dec 23 10:14 db588b34-2fcb-43aa-aeaf-657a934102da -> ../../vda1
sub0@dbxnode:~$
```

Κάθε διαμέρισμα ενός οποιουδήποτε δίσκου έχει ένα μοναδικό αναγνωριστικό μήκους 128 bits, που ονομάζεται UUID (από το Universally Unique IDentifier). Στις γραμμές του αρχείου /etc/fstab, με βάση τις οποίες γίνεται η προσάρτηση (mounting) των διαμερισμάτων, καλό είναι να βάζουμε τα σταθερά UUIDs κι όχι τα δυναμικά device names. (Όσο ένα διαμέρισμα υφίσταται διατηρεί αναλλοίωτο το UUID του, ανεξάρτητα από τη φυσική θέση του δίσκου και τη δυναμική ονομασία που του αποδίδει το λειτουργικό σύστημα.) Ένας τρόπος για να μαθαίνουμε τα UUIDs των διαμερισμάτων είναι με μια ματιά στα περιεχόμενα του καταλόγου /dev/disk/by-uuid. Στο screenshot, το UUID που μας ενδιαφέρει αποτελεί symbolic link προς το /dev/vdb1 (ή προς το ../../vdb1, σε σχέση με τον κατάλογο /dev/disk/by-uuid). Καλό είναι να επιλέξουμε το UUID με το ποντίκι και να το αντιγράψουμε με δεξί κλικ και Copy.

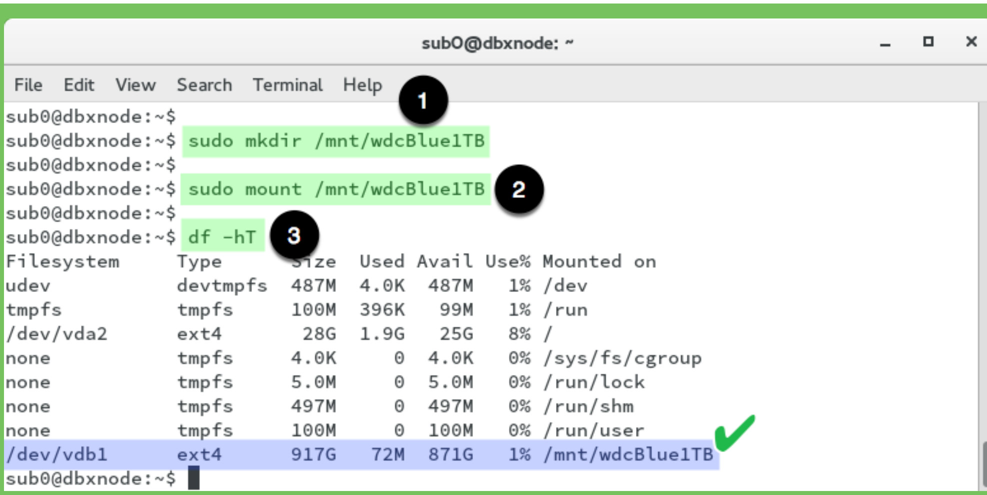


```
sub0@dbxnode: ~
File  Edit  View  Search  Terminal  Help
sub0@dbxnode:~$
sub0@dbxnode:~$ sudo nano /etc/fstab
```

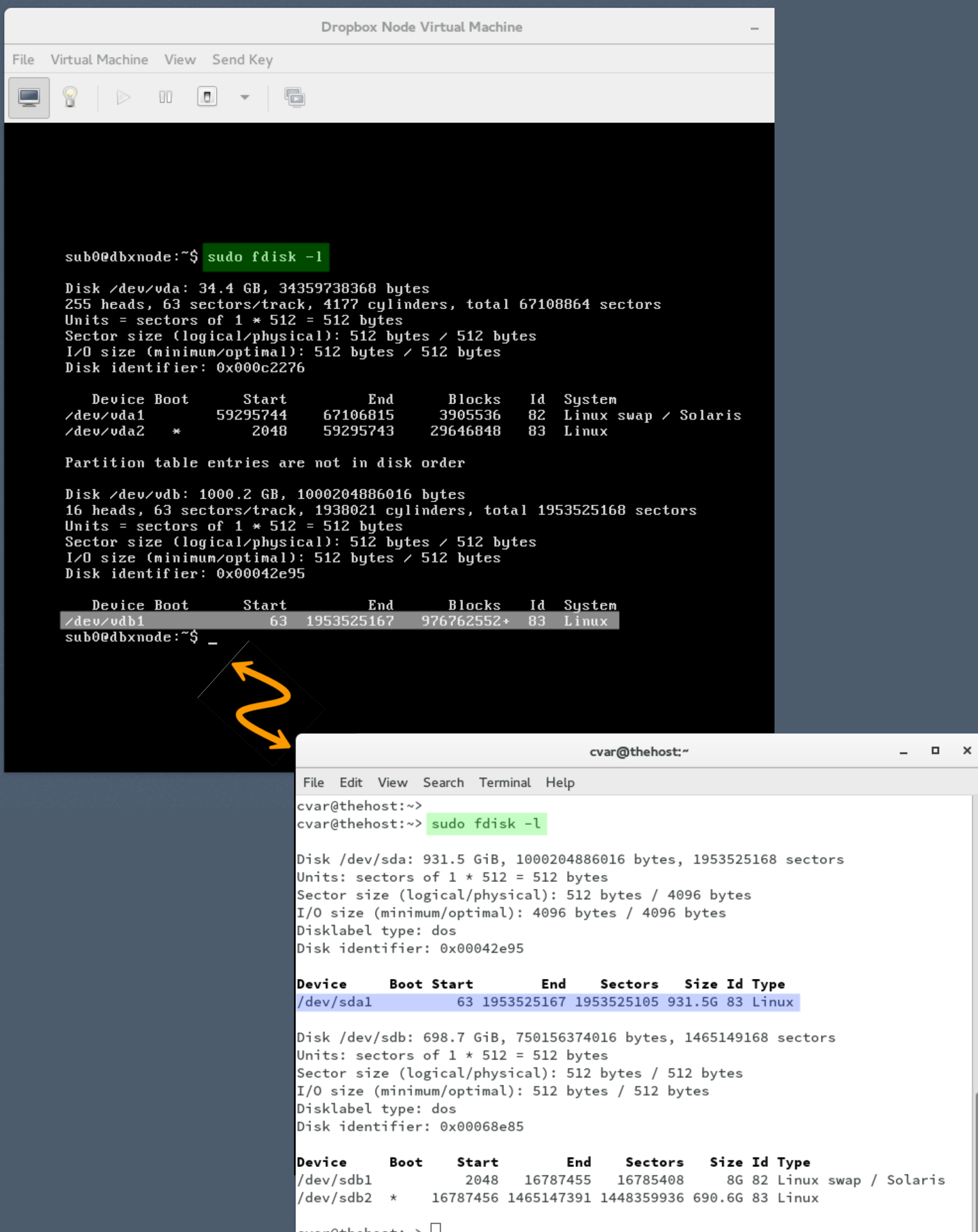
Σειρά έχει η τροποποίηση του αρχείου fstab στον κατάλογο /etc, το οποίο ανοίγουμε με δικαιώματα υπερχρήστη και με τη βοήθεια του nano. Θα προσθέσουμε στο αρχείο μία μόνο γραμμή, ώστε το νέο διαμέρισμα να προσαρτάται αυτόματα κατά την εκκίνηση του λειτουργικού.



Ιδού η γραμμή που εμείς προσθέσαμε στο /etc/fstab. Στη δική σας περίπτωση θα διαφέρει το UUID, ο κατάλογος προσάρτησης (/mnt/wdcBlue1TB) – δεν αποκλείεται και το είδος του συστήματος αρχείων (ext4).



Αφού κάναμε την προσθήκη μας στο fstab, είναι ώρα να προσαρτήσουμε τη νέα κατάτμηση. Ξεκινάμε δημιουργώντας τον κατάλογο προσάρτησης (1) κι αμέσως μετά πραγματοποιούμε την ίδια την προσάρτηση (2). Θέλουμε να βεβαιωθούμε ότι όλα έχουν πάει καλά, γι' αυτό και παρατηρούμε την έξοδο του df (3). Η τελευταία γραμμή μάς καθησυχάζει, μας χαροποιεί και μας γεμίζει αισιοδοξία για τη ζωή!



Το νέο διαμέρισμα που δημιουργήσαμε και προσαρτήσαμε είναι ορατό τόσο από από το guest OS (Ubuntu Server, αριστερά), όσο κι από το host OS (openSUSE, δεξιά). Καλό αυτό, ωστόσο όταν το VM είναι ενεργό σκοπεύουμε να γράφουμε και να διαβάζουμε δεδομένα μόνον από το guest OS.


ΔΕΚΕΜΒΡΗΣ
17
ΠΕΜΠΤΗ
ΧΡΙΣΤΟΦΟΡΕ, ΣΥΓΧΑΡΗΤΗΡΙΑ ΓΙΑ ΤΗ ΝΕΑ ΣΟΥ ΤΑΙΝΙΑ...
ΑΜΕΙΟ
ΑΛΛΟΣ ΚΟΣΜ
ΠΡΕΜΙΕΡΑ
ΜΕΤΑΞΥ ΜΑΣ ΟΜΩΣ ΤΩΡΑ, ΔΕ ΘΑ ΓΟΥΣΤΑΡΕΣ ΑΠΟΨΕ ΝΑ ΔΕΙΣ ΣΤΑΡΓΟΥΟΡΣ;
ΜΠΛΙΝΚ
ΑΥΤΑ ΠΟΥ ΛΕΣ ΕΙΝΑΙ ΤΙ; ΠΡΟΣΒΑΜΕΙΣ ΣΤΑΜΑΤΑ ΝΑ ΜΕ!..
ΟΣ
...ΧΜΜΜ...
TiaNOS

deltahacker.gr